Faculteit Wetenschappen
Vakgroep Wiskunde

Undecidability problems and diophantine sets over polynomial rings and function fields

Claudia Degroote

Promotors: Jeroen Demeyer and Jan Van Geel

Faculteit Wetenschappen
Vakgroep Wiskunde

Undecidability problems and diophantine sets over polynomial rings and function fields

Claudia Degroote

Promotors: Jeroen Demeyer and Jan Van Geel

Contents

Thanks

First of all, I would like to thank my advisors, Jan Van Geel and Jeroen Demeyer.

Jan has now been my advisor for my bachelor project, master thesis and PhD thesis, and I can not express enough gratitude for supporting me and making time for me through these past years. He is my role model of a mathematician, and I thank him a lot for all the good advice he gave me and the insightful discussions we had.

I am also very grateful to my second advisor, Jeroen. We worked together a lot, and I appreciate all the help and support he gave me, his critical perception and of course his energetic enthusiasm. Also thank you for being my traveling companion so many times!

I was lucky to do my PhD together with the other algebra girls, Sofie Beke, Elizabeth Callens and Lien Boelaert. Thank you for the many lively four o'clock breaks that we shared. We could not always help each other with math, but at least we could talk about the same struggles we went through.

I also want to thank everyone else from the algebra group and the colleagues of the mathematics department.

People who also deserve thanks are Xavier Vidaux and Thanases Pheidas. Thank you for inviting me, for your hospitality and the interesting mathematical discussions.

Special thanks go to my mother, who encouraged me and gave me all the chances

I needed to study. You stimulated me to take an interest in almost every subject, and I am glad for the broad view it gave me. I'm also thankful to my sisters and brothers, Marjolein, Johanna, Adriaan, Boudewijn, Annelies and Alexander. Especially to Johanna, for being my best friend and for trying out almost all vegetarian restaurants of Ghent with me. To Adriaan, for being my cool technology-nerd brother. And to "de kleintjes", you are probably wondering when we will stop calling you that, but you know that I adore you.

And finally to Wim, for being with me always, believing in me and giving the best motivating talks whenever I doubted myself. I cherish every day of the wonderful life we share. So thanks for loving me, 'cause you're doing it perfectly.

Introduction

Hilbert's Tenth Problem is one of the 23 mathematical problems that Hilbert drew up in 1900. Some of them he presented in his famous address at the Paris conference of the International Congress of Mathematics in 1900. He intended his problems to be studied in the upcoming century. The complete list of 23 problems was published later, for example in [Hil00]. The original statement of Hilbert's Tenth Problem reads as follows.

Entscheidung der Lösbarkeit einer Diophantischen Gleichung. Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

Or translated.

Determination of the solvability of a diophantine equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

In modern terminology, we would say that Hilbert's Tenth Problem asks for an algorithm with input a polynomial over $\mathbb{Z}$ in any number of variables, and output "yes" if the given polynomial has an integer solution and "no" if the polynomial has no integer solution. In 1970, Matiyasevich proved the following theorem, building on earlier work of Davis, Putnam and Robinson.

Theorem (DPRM-theorem). *A set $A \subseteq \mathbb{Z}^k$ is recursively enumerable if and only if A is diophantine over $\mathbb{Z}$.*

We call this the DPRM-theorem, from this theorem follows the negative answer to Hilbert's Tenth problem, so there exists no algorithm that decides whether diophantine equations over $\mathbb{Z}$ have a solution.

Hilbert's Tenth Problem, as well as the stronger DPRM-theorem can be formulated for other rings and fields (see Section 2.1 and 5.1). In this thesis we present such results: we prove the negative answer to Hilbert's Tenth Problem for rational function fields in one variable over a p-adic field (i.e. a finite extension of some $\mathbb{Q}_p$). Concerning the DPRM-theorem, we prove that recursively enumerable sets that are recursively enumerable for every recursive presentation, are diophantine for the polynomial ring in one variable over certain algebraic extensions of $\mathbb{Q}$.

A good overview of known results and open problems concerning Hilbert's Tenth Problem can be found in the survey articles [Phe94] and [PZ00]. Also interesting surveys that explore relations with other questions in arithmetic and algebraic geometry are [Maz94] and [Shl00]. There are also two good introductory texts on Hilbert's Tenth Problem by Poonen, namely [Poo03] and [Poo08].

The results known so far of undecidability of diophantine equations for a domain R, all reduce to the undecidability result for $\mathbb{Z}$. To do this reduction, one tries to find a diophantine model of the integers in R. For rational function fields $K(t)$ over a field K, it suffices to give a diophantine definition of the valuation ring of v_∞. With this definition, one uses elliptic curves to build such a diophantine model of the integers. This method was first used by Denef ([Den78a]) in characteristic zero, in general the result can be stated as follows.

Theorem ([PZ00, Theorem 2.3]). *Let K be a field and let K_0 denote the prime subfield of K. Let t be a transcendental element over K. Suppose that there exists a diophantine definition $\psi(x)$ such that the following hold:*

1. *for every $x \in K_0(t)$ such that $v_\infty(x) \geq 0$, $\psi(x)$ holds;*
2. *for every $x \in K(t)$ such that $\psi(x)$ holds, we have $v_\infty(x) \geq 0$.*

Then diophantine equations over $K(t)$ are undecidable.

Denef used this to prove diophantine undecidability for $K(t)$, with K a real field. In [KR95], Kim and Roush proved undecidability for $K(t)$, with K a subfield of a p-adic field, with odd residue characteristic. We improved their result in [DD12], and gave a proof of diophantine undecidability for $K(t)$, with K a p-adic field that is possibly dyadic. We used this to prove undecidability for $K(t)$, with K an algebraic subfield of a p-adic field, also without assumptions on the residue characteristic. For positive characteristic p, diophantine undecidability for $K(t)$, K a finite field of characteristic p, was proved by Pheidas in [Phe91] (p odd), and Videla in [Vid94] ($p = 2$). Kim and Roush proved in [KR92] diophantine undecidability for $\mathbb{C}(t_1, t_2)$. It is an open problem whether diophantine equations over $\mathbb{C}(t)$ are undecidable.

Now let $R[t]$ be the polynomial ring in one variable over a domain R of characteristic 0. In [Den78a], Denef proved that Hilbert's Tenth Problem for $R[t]$ with coefficients in $\mathbb{Z}[t]$ is undecidable. Later, he also proved the result for a domain of positive characteristic p in [Den79] (with the coefficients of the diophantine equations in $(\mathbb{Z}/p\mathbb{Z})[t]$).

If R is a recursive ring, one can consider the stronger result that recursively enumerable sets are diophantine. Much less is known about this. First, there is the result of Denef that recursively enumerable sets are diophantine for the polynomial ring $\mathbb{Z}[t]$ (see [Den78b]). This method has been generalized by Zahidi, who proved the equivalence in [Zah99] for $O_K[t_1, \ldots, t_n]$ with O_K the ring of integers in a totally real number field K, and by Demeyer in [Dem10] for $R[t]$ with R a recursive subring of a number field. In characteristic p, Demeyer proved for $K[t]$, with K a recursive algebraic extension of a finite field, that sets that are recursively enumerable for every recursive presentation are diophantine, using his result in [Dem07b] that r.e. sets are diophantine for $\mathbb{F}_q[t]$. We proved that recursively enumerable sets that are recursively enumerable for every recursive presentation, are diophantine for $L[t]$, with $L/\mathbb{Q}$ an automorphism-recursive algebraic extension, that can be embedded in a real field or in a p-adic field.

Overview of the thesis

Part I: Hilbert's Tenth Problem for rational function fields

In part I we prove diophantine undecidability for the rational function field $K(t)$ over a p-adic field K (i.e. a finite extension of some $\mathbb{Q}_p$) and also over an algebraic subfield K of a p-adic field. This generalizes a result of Kim and Roush, who proved in [KR95] diophantine undecidability for rational function fields over subfields of a p-adic field with odd residue characteristic. In this thesis, we adapt their methods by working more in the context of the theory of quadratic forms, and we give a unified proof that handles both residue characteristic p odd and $p = 2$.

Part I starts with two preliminary chapters. In the first, we recall the definition of a valuation and some basic properties. The valuations that we work with mostly in this thesis, are the p-adic valuations and the valuations on a rational function field $K(t)$ that are trivial on K (although certain valuations extending the p-adic valuation to $K(t)$, which we consider in Section 1.3, come implicitly into the proof of our Main Theorem). We also introduce Newton polygons, a geometric object that gives the valuations of the roots of a polynomial. In the second chapter, we give an introduction to Hilbert's Tenth Problem, hereby concentrating on rational function fields. We give Denef's proof that reduces diophantine undecidability for $K(t)$ to giving a diophantine definition of the valuation ring of v_∞ in $K(t)$, for $\operatorname{char} K = 0$. In this way, we present in this thesis a completely self-contained proof of our result of diophantine undecidability for $K(t)$, with K a p-adic field. To

conclude, we compare the known results on undecidability for rational function fields.

In our diophantine definition of the valuation ring of v_∞ in $K(t)$, quadratic forms play an important role. Namely, we need to be able to prove whether a certain class of 7-dimensional quadratic forms, whose coefficients depend on a given rational function, is isotropic. Therefore, Chapter 3 concentrates solely on quadratic forms, first giving some introduction, and then the build-up to our Main Theorem 3.3.1, which says that if $g \in K[t]$ has a particular Newton polygon then a certain 7-dimensional quadratic form q involving g is isotropic over $K(t)$. Our proof follows some of the structure of the proof by Kim and Roush, but they prove a lot of the theorems in their article about quadratic forms by reducing to the residue field. Since this is a rational function field over a finite field of odd characteristic, this allows them to use quadratic reciprocity, and then lift the result back, using Hensel's Lemma. Since we wanted a proof that also works in residue characteristic 2, we could not use this technique. But actually, it is more natural to look at the polynomials over the p-adic field K, instead of at the reduction over the residue field. So, in Section 3.2, we define a type of quadratic reciprocity symbol for polynomials over K, and we verify a quadratic reciprocity law for this symbol.

In [KR95], Kim and Roush also prove that the quadratic form q is isotropic over rational function fields over algebraic subfields of nondyadic p-adic fields. In their proof, they go to a finite extension of K, in which they get rid of the dyadic primes. So they only give a diophantine definition of the valuation ring of v_∞ for subfields of nondyadic p-adic fields that satisfy certain conditions. Since they also prove that every subfield of a nondyadic p-adic field has such a finite extension with extra conditions, this is enough to prove Hilbert's Tenth Problem for $K(t)$, with K a subfield of a nondyadic p-adic field. Using our previous result for p-adic fields, we also simplify and generalize this proof so that it holds for all primes p. In our proof, going to a finite extension is no longer necessary, so we are able to give a diophantine definition of the valuation ring of v_∞ for all rational function fields in one variable over an algebraic subfield of a p-adic field. This is done in Chapter 4, where we use our result on the isotropy of q to give a diophantine definition of the predicate "$v_\infty(x)$ is even" for $x \in K(t)$. This can then be reformulated to a diophantine definition of "$v_\infty(x) \geq 0$", which is implicitly done in Theorem 4.1.5.

Our result on diophantine undecidability for $K(t)$, with K a p-adic field, was published in [DD12].

Part II: Diophantine sets over polynomial rings

Our starting point in this part is the work that Demeyer did in his PhD thesis (see [Dem07a]) for polynomial rings over $\mathcal{O}_L$, with L a totally real algebraic extension of $\mathbb{Q}$. We will examine when recursively enumerable sets are diophantine for the polynomial ring $L[t]$, with $L/\mathbb{Q}$ a recursive, algebraic extension. First of all, whether a set $\mathcal{S} \subseteq L[t]$ is recursively enumerable (r.e.) could depend on the chosen recursive presentation of $L[t]$. However, diophantine sets are r.e. for every recursive presentation. Furthermore, a diophantine set is invariant under $\mathrm{Aut}(L/F)$, with $F/\mathbb{Q}$ the finite extension generated by the defining equation of the diophantine set. So only recursively enumerable sets $\mathcal{S} \subseteq L[t]$ that are recursively enumerable for every recursive presentation of $L[t]$ and that are invariant under the automorphism group of some finite extension of $\mathbb{Q}$, can be diophantine. In Section 6.3, we show that these two conditions that r.e. sets would have to satisfy, are actually equivalent. Namely, a recursively enumerable set $\mathcal{S}$ is recursively enumerable for every recursive presentation if and only if there exists a finite extension $F/\mathbb{Q}$ such that $\mathcal{S}$ is invariant as a set under $\mathrm{Aut}(L/F)$.

To prove the main result of this part, namely that recursively enumerable sets that are r.e. for every recursive presentation are diophantine for $L[t]$, with $L/\mathbb{Q}$ a recursive, algebraic extension, we needed an extra condition on the automorphisms of L. This led us to the definition of an automorphism-recursive field. In an automorphism-recursive field L, given an element $\alpha \in L$, we can compute the number of roots in L of the minimal polynomial of α over F, and we know how many of these roots are $\mathrm{Aut}(L/F)$-conjugate to α. Examples of an automorphism-recursive field include Galois extensions $L/\mathbb{Q}$ and the real closure of $\mathbb{Q}$. We proved some essential properties that an automorphism-recursive field has, for example, given an element $\alpha \in L$, we do not only know the number of $\mathrm{Aut}(L/F)$-conjugates to α, but it is also possible to compute this set. To get some more intuition for the concept of an automorphism-recursive field, we also constructed fields that have one of these properties but that are not automorphism-recursive. Another important property that an automorphism-recursive field has,

is that we can effectively compute a pair of polynomials over a number field F in L that characterizes the $\mathrm{Aut}(L/F)$-conjugates of an element $\alpha \in L$. We then used these polynomials to encode the elements of the recursively enumerable set $\mathcal{S}$ with $\mathrm{Aut}(L/F)(\mathcal{S}) = \mathcal{S}$ in a diophantine way. Another thing that we needed to prove that our definition of $\mathcal{S}$ is diophantine, is that $\mathbb{Z}[t]$ is diophantine over $L[t]$.

In Theorem 7.2.4 we prove the main result of this part. If $L/\mathbb{Q}$ is automorphism-recursive and $\mathbb{Z}[t]$ is diophantine over $L[t]$, then recursively enumerable sets in $L[t]$ that are recursively enumerable for every recursive presentation, are diophantine.

From [Dem10] follows that $\mathbb{Z}[t]$ is diophantine over $L[t]$ if the predicate "$\deg a \leq \deg b$" for $a, b \in L[t] \setminus \{0\}$ is diophantine. In Chapter 7.1, we give a diophantine definition of the degree in the case that L can be embedded in $\mathbb{R}$ and in the case that L can be embedded in a p-adic field.

We prepared a paper on this work together with Jeroen Demeyer.

Part I

Hilbert's Tenth Problem for rational function fields

Chapter 1

Valuations

In this chapter we highlight the valuations that we need in this thesis, namely valuations on a rational function field in one variable and p-adic valuations. With a polynomial g in one variable over a field K with a discrete valuation, we can associate a geometric object, the Newton polygon of g. The slopes of the edges of this polygon are related to the valuations of the roots of the polynomial g. For each possible slope we can also define a certain "sloped polynomial" ring R and a prime ideal P. The localization of this ring R at P then turns out to be the valuation ring of a valuation on $K(t)$, that restricts to the valuation on K.

1.1 Valuations

We assume the reader is familiar with valuations, for more theory, we refer to [EP05].

Definition 1.1.1. A *(non-archimedean) rank* 1 *valuation* v on a field K is a map $v : K \to \mathbb{R} \cup \{\infty\}$ such that for all $a, b \in K$:

1. $v(a) = \infty \Leftrightarrow a = 0$,
2. $v(ab) = v(a) + v(b)$,

3. $v(a+b) \geq \min\{v(a), v(b)\}$.

A valuation v is nontrivial if there exists an $a \in K^*$ such that $v(a) \neq 0$. A valuation v is *discrete* if the value group $v(K^*)$ is isomorphic to $\mathbb{Z}$.

Unless stated otherwise, the word “valuation" will always mean a nontrivial non-archimedean rank 1 discrete valuation.

From the definition easily follows that if $v(a) \neq v(b)$ then $v(a+b) = \min\{v(a), v(b)\}$.

We denote with $\mathcal{O}_v$ the *valuation ring*

$$\mathcal{O}_v = \{a \in K \mid v(a) \geq 0\},$$

with unique maximal ideal

$$\mathcal{M}_v = \{a \in K \mid v(a) > 0\},$$

and *residue field* $\overline{K} = \mathcal{O}_v/\mathcal{M}_v$. Since v is discrete, $\mathcal{O}_v$ is a principal ideal domain. We call an element $\pi \in \mathcal{O}_v$ a *uniformizer* for v, if π is a generator of the maximal ideal $\mathcal{M}_v$. We call two valuations v and w on a field K *equivalent* if they have the same valuation ring.

Since a valuation defines a metric on K (by defining the distance $d(a,b)$ between points $a, b \in K$ as $d(a,b) = e^{-v(a-b)}$), we can consider the completion $\hat{K}$ of K with respect to this metric. The valuation v extends canonically to $\hat{K}$, we denote this extension also with v. For the valuation ring $\hat{\mathcal{O}}_v$ of the completion and its maximal ideal $\hat{\mathcal{M}}_v$, we have that $\hat{\mathcal{O}}_v/\hat{\mathcal{M}}_v \cong \mathcal{O}_v/\mathcal{M}_v$. If K is complete with respect to a valuation v, then Hensel's Lemma holds.

Theorem 1.1.2 (Hensel's Lemma, [EP05, Theorem 4.1.3]). *For all $f \in \mathcal{O}_v[x]$ and $a \in \mathcal{O}_v$ such that $v(f(a)) > 2v(f'(a))$, there exists a $b \in \mathcal{O}_v$ such that $f(b) = 0$ and $v(b-a) > v(f'(a))$.*

More generally, we call a valued field (K, v) *henselian* if Hensel's Lemma holds.

Definition 1.1.3. Let L/K be a field extension, and w a valuation on L that extends the valuation v on K. Then $e(w/v) = [w(L^*) : v(K^*)]$ is called the *ramification degree*, and $f(w/v) = [\overline{L} : \overline{K}]$ the *residue degree*.

On the field of the rational numbers $\mathbb{Q}$, we define for every prime number p the *p-adic valuation* v_p. This valuation is defined for every $q \in \mathbb{Q}^*$ by writing $q = p^n \frac{\alpha}{\beta}$, with $n, \alpha, \beta \in \mathbb{Z}$, α, β coprime to p, and letting

$$v_p(q) = n.$$

The completion of $\mathbb{Q}$ at v_p is known as the field of the p-adic numbers $\mathbb{Q}_p$.

Let K be a number field. Then every equivalence class of valuations of K (also called a prime $\mathfrak{p}$ of K), determines a prime ideal in the ring of integers $\mathcal{O}_K$ (and vice versa). These are also called the finite primes of K. Since equivalent valuations give rise to the same topology on K, the completion of K at a prime $\mathfrak{p}$ is well-defined, and we denote it with $K_\mathfrak{p}$. If p is the prime below $\mathfrak{p}$ (this means that $\mathfrak{p} \cap \mathbb{Z}$ is the prime ideal generated by p, we also denote this with $\mathfrak{p} \mid (p)$), then $K_\mathfrak{p}$ is a finite extension of $\mathbb{Q}_p$. Its residue field is the finite field $\mathbb{F}_{p^f}$, with f the residue degree of $\mathfrak{p}$ over p.

There are also infinite primes on K, given by the embeddings $\varphi : K \to \mathbb{C}$. These split into two classes, namely the real primes, given by embeddings $\varphi : K \to \mathbb{R}$ (so the completion is isomorphic to $\mathbb{R}$), and the complex primes, induced by pairs of complex conjugated non-real embeddings $K \to \mathbb{C}$ (in this case the completion is isomorphic to $\mathbb{C}$).

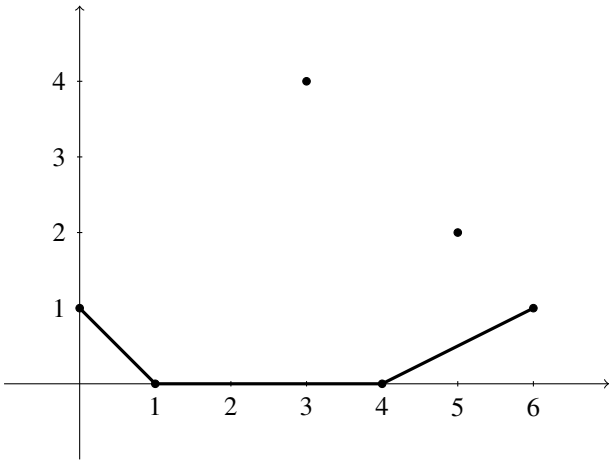
1.2 Newton polygons

Let K be a field with a discrete henselian valuation v. Let $\mathcal{O}$ denote the valuation ring.

Definition 1.2.1. Let $f(t) = a_0 + a_1 t + \ldots + a_d t^d$ be a polynomial over K with $a_0 a_d \neq 0$. The *Newton polygon* of f is the lower convex hull of the points $(i, v(a_i))$ in $\mathbb{R}^2$. A *vertex* of the Newton polygon is a point $(i, v(a_i))$ where two edges of a different slope meet. We call i the *degree* of the vertex $(i, v(a_i))$.

Example 1.2.2. Consider the polynomial $f(t) = p + (-1 + p^3)t + p^4 t^3 + (-1 - p^3)t^4 + p^2 t^5 - p t^6 = \sum_{i=0}^{6} a_i t^i$, with p a prime number. The following figure shows the points $(i, v_p(a_i))$, $i \in \{0, \ldots, 6\}$ and the Newton polygon of f for the p-adic

valuation. Remark that $f = (-p)(t-p)(t^3+p^2t+1)(t^2+\frac{1}{p})$.



The Newton polygon of a polynomial consists of a sequence of edges with strictly increasing slopes, for which the following holds.

Theorem 1.2.3 ([Neu92, Chapter II, Theorem 6.3 and 6.4]). *Let K be a field with a discrete henselian valuation v. Let $f(t) = a_0 + a_1t + \ldots + a_dt^d$ be a polynomial over K with $a_0a_d \neq 0$. Denote the unique extension of v on the splitting field of f also by v. If $(r, v(a_r)) - (s, v(a_s))$ is an edge of the Newton polygon of f with slope m, then f has exactly $s-r$ roots $\alpha_1, \ldots, \alpha_{s-r}$ with valuation $v(\alpha_1) = \cdots = v(\alpha_{s-r}) = -m$. If the slopes of the Newton polygon of f are $m_1 < \ldots < m_k$ then*

$$f(t) = a_d \prod_{j=1}^{k} f_j(t), \tag{1.1}$$

with $f_j(t) = \prod_{v(\alpha_i)=-m_j}(t-\alpha_i) \in K[t]$.

Definition 1.2.4. We define *the factorization of f according to the slopes* to be the expression $a_d \prod_{j=1}^{k} f_j(t)$ in (1.1). Note that the polynomials $f_j(t)$ are not necessarily irreducible over K. The Newton polygon of each $f_j(t)$ has exactly one edge of slope m_j.

Lemma 1.2.5. *Let $f(t) = \sum_{k=0}^{d} a_kt^k$ be a polynomial with $a_0a_d \neq 0$, whose Newton polygon has only one edge. Let $m := \frac{v(a_d)-v(a_0)}{d}$ be the slope. Let $\alpha \in K$. Then*

$$v(a_k\alpha^k) \geq k(m + v(\alpha)) + v(a_0),$$

with $k = 0, \ldots, d$.

Proof. Since the Newton polygon of f has only one edge, we have that $\frac{v(a_k)-v(a_0)}{k} \geq m$, for all $k = 0, \ldots, d$, from which the Lemma follows. □

The following Proposition will be very useful in the proof of our Main Theorem 3.3.1.

Proposition 1.2.6. *Let K be a field with a discrete henselian valuation v and let $\alpha \in K$. Let f be a polynomial over K of even degree with $f(0) \neq 0$. Assume that the Newton polygon of f has only one edge, let m be the slope. Assume that $m \neq -v(\alpha)$ and let $N \in \mathbb{N}$ be such that*

$$N > \frac{v(4)}{|m + v(\alpha)|}. \tag{1.2}$$

Assume that f is of the form

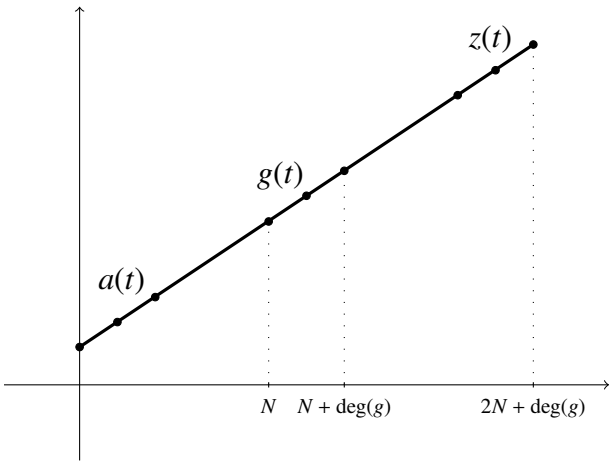
$$f = a(t) + g(t)t^N + z(t)t^{2N+\deg g - \deg z},$$

where a, g and z are polynomials over K. Assume that $\deg(g)$ and $\deg(z)$ are even and that $\deg(a) \leq \deg(g) + N$ and $\deg(z) \leq \deg(g) + N$.

If $m < -v(\alpha)$, then $f(\alpha) = z(\alpha)$ in K^*/K^{*2}. If $m > -v(\alpha)$, then $f(\alpha) = a(\alpha)$ in K^*/K^{*2}.

Remark that we can always take $N = 1$ in (1.2) if the residue characteristic is different from 2.

The following figure shows the Newton polygon of an example of such an f.



Proof. Let $d = 2N + \deg(g)$ be the degree of f. Suppose first that the slope m of f is strictly smaller than $-v(\alpha)$. Let $c := z(\alpha)\alpha^{2N+\deg g-\deg z}$. The leading term of c is the monomial of strictly lowest valuation in $f(\alpha)$. Note that $v(c) = d(m + v(\alpha)) + v(f(0))$. We then have that

$$c^{-1}f(\alpha) = c^{-1}a(\alpha) + c^{-1}g(\alpha)\alpha^N + 1.$$

Using Lemma 1.2.5 and $\deg(a) \leq \deg(g) + N$, the inequality (1.2) implies

$$\begin{aligned} v(a(\alpha) + g(\alpha)\alpha^N) &\geq (\deg g + N)(m + v(\alpha)) + v(f(0)) = (-N)(m + v(\alpha)) + v(c) \\ &= N|m + v(\alpha)| + v(c) > v(4) + v(c). \end{aligned}$$

Therefore,

$$v(c^{-1}f(\alpha) - 1) > v(4).$$

By Hensel's Lemma (see Theorem 1.1.2) applied to the polynomial $x^2 - (c^{-1}f(\alpha))$, we find that $c^{-1}f(\alpha)$ is a square. Since $\alpha^{2N+\deg g-\deg z}$ is a square, it follows that $z(\alpha)$ is in the same square class as c, hence in the same square class as $f(\alpha)$.

If the slope m of f is strictly bigger than $-v(\alpha)$, we let $c := a(\alpha)$. The constant term of c is the monomial of strictly lowest valuation in $f(\alpha)$. We then have that

$$c^{-1}f(\alpha) = 1 + c^{-1}g(\alpha)\alpha^N + c^{-1}z(\alpha)\alpha^{d-\deg z}.$$

Using Lemma 1.2.5 and $\deg(z) \leq \deg(g) + N$, the inequality (1.2) implies

$$\begin{aligned} v(g(\alpha)\alpha^N + z(\alpha)\alpha^{d-\deg z}) &\geq N(m + v(\alpha)) + v(f(0)) \\ &= N|m + v(\alpha)| + v(c) > v(4) + v(c). \end{aligned}$$

Therefore,

$$v(c^{-1}f(\alpha) - 1) > v(4).$$

As before, we find that $c^{-1}f(\alpha)$ is a square; hence $f(\alpha)$ is in the same square class as $c = a(\alpha)$. □

1.3 Valuations on $K(t)$

Let $K(t)$ be the rational function field in one variable over a field K. With every irreducible polynomial $p(t) \in K[t]$, we can associate a valuation v_p as follows.

Every $f \in K(t)$ can be written as $f = p^a \frac{f_1}{f_2}$ with $a \in \mathbb{Z}$, $f_1, f_2 \in K[t]$, and f_1, f_2 coprime to p, and then we define

$$v_p(f) = a.$$

There is also a valuation associated to the degree, namely

$$v_\infty\left(\frac{f_1}{f_2}\right) = \deg f_2 - \deg f_1.$$

These are all the valuations on $K(t)$ that are trivial on K.

Let K be a p-adic field, that is, a finite extension of $\mathbb{Q}_p$ for some prime p. We denote the valuation with v and the valuation ring with $\mathcal{O}$, we fix a uniformizer π (a generator of the maximal ideal $\mathcal{M}$ in $\mathcal{O}$). Denote the residue field with k, this is a finite field of characteristic p. We work in a fixed algebraic closure $\bar{K}$ of K and we normalize the valuation on K and all its finite extensions such that $v(\pi) = 1$. This means that for $\beta \in \mathbb{N} \setminus \{0\}$, $v(\sqrt[\beta]{\pi}) = \frac{1}{\beta}$ in $K(\sqrt[\beta]{\pi})$. Remark that from [EP05, Theorem 4.1.3] follows that v extends uniquely to $\bar{K}$.

Let $m \in \mathbb{Q}$. We can define a valuation on $K(t)$ that is not the trivial valuation on K, as follows. For $f = a_0 + a_1 t + \cdots + a_n t_n \in K[t] \setminus \{0\}$, define

$$v_m(f) = \min_i \{v(a_i) + im\}. \tag{1.3}$$

For $f, g \in K[t] \setminus \{0\}$, let $v_m(f/g) = v_m(f) - v_m(g)$. From [EP05, Theorem 2.2.1] follows that v_m is a valuation on $K(t)$ that extends v.

If $m = 0$, this valuation is also known as the Gauss valuation and denoted with v_G. From [EP05, Corollary 2.2.2] follows that for the reduction at v_G, $\bar{t}$ is transcendental over k, and for the residue field we have that $\overline{K(t)} = k(\bar{t})$. Similarly, one can prove the following.

Lemma 1.3.1. *Let K be a field, with a discrete valuation $v : K \to \mathbb{Z} \cup \{\infty\}$ and uniformizer π, let $m \in \mathbb{Q}$. Let d be the denominator of m. Then there is exactly one extension w of v to $K(\pi^m)(t)$ such that $w(t) = m$ and $\overline{\pi^{-m}t}$ is transcendental over k. For this w, the residue field is $k(\overline{\pi^{-m}t})$ and the value group is $\frac{1}{d}\mathbb{Z}$.*

We actually want to consider v_m on $K(t)$, instead of going to the extension $K(\pi^m)(t)$. So define for $m \in \mathbb{Q}$

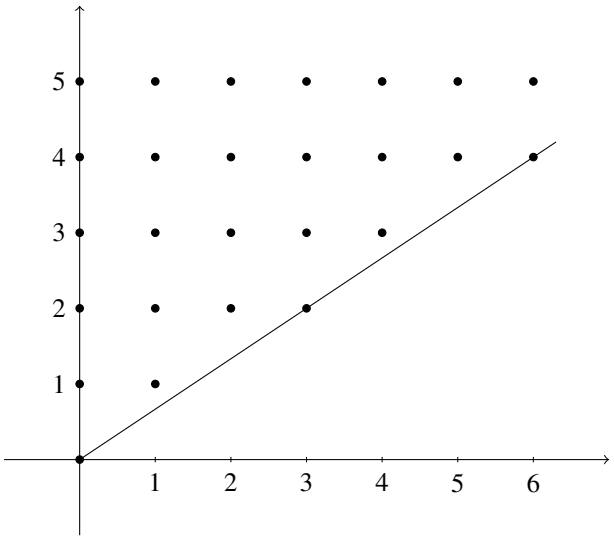
$$R_m := \sum_{\{(\alpha,\beta)\in\mathbb{Z}^2 | \beta\geq 0 \ \wedge \ \alpha\geq m\beta\}} (\pi^\alpha t^\beta)O.$$

Clearly, R_m is an O-module in $K[t]$, but one can check that it is actually a subring. Consider the ideal

$$P_m = \sum_{\{(\alpha,\beta)\in\mathbb{Z}^2 | \beta\geq 0 \ \wedge \ \alpha> m\beta\}} (\pi^\alpha t^\beta)O$$

in R_m. Let d be the denominator of m and $u := \pi^{md}t^d$. From now on, a line over an element of R_m denotes reduction modulo P_m. The quotient ring R_m/P_m is $k[\overline{u}]$ (the variable $\overline{u}$ is precisely the reduction of the element $u = \pi^{md}t^d$), so P_m is a prime ideal in R_m.

In the following figure we visualize the ring R_m and its prime ideal P_m for $m = 2/3$. We let a monomial $\pi^\alpha t^\beta$ correspond to the point (β, α). The points drawn correspond to the monomials in R_m, the points that lie strictly above the line correspond to the monomials in P_m.



Lemma 1.3.2. *Let $m \in \mathbb{Q}$, let d be the denominator of m and $u = \pi^{md}t^d$. Let $f(t) = a_0 + a_1t + \ldots + a_nt^n$ be a polynomial over K with $a_0a_n \neq 0$. Assume that the Newton polygon of f has only one edge and let μ be the slope.*

(i) *If $\mu > m$, then $\pi^{-v(a_0)} f \in R_m$ and $\overline{\pi^{-v(a_0)} f} = \overline{\pi^{-v(a_0)} a_0} \neq 0$.*

(ii) *If $\mu < m$, then, for every $B \in d\mathbb{Z}$ such that $B \geq n$, $\pi^{-v(a_n)+Bm} t^{B-n} f \in R_m$. With $B = db$, we have that $\overline{\pi^{-v(a_n)+Bm} t^{B-n} f} = \overline{\pi^{-v(a_n)} a_n} \overline{u}^b$.*

(iii) *If $\mu = m$, then $\pi^{-v(a_0)} f \in R_m$ and $\overline{\pi^{-v(a_0)} f} = \overline{\pi^{-v(a_0)} a_0} + \cdots + \overline{\pi^{-v(a_0)} a_n} \overline{u}^{n/d}$ is a polynomial with constant term nonzero and of degree n/d in $\overline{u}$.*

Proof. Since the Newton polygon of f has only one slope, it follows that $v(a_i) \geq i\mu + v(a_0)$ for all $i = 0, \ldots, n$ and $v(a_n) = n\mu + v(a_0)$.

(i) Let $\mu > m$. We then have that $v_{-m}(f) = \min_i\{v(a_i) - im\} = v(a_0)$. For $k > 0$, we have that

$$v(\pi^{-v(a_0)} a_k) \geq -v(a_0) + (k\mu + v(a_0)) > km.$$

So $\pi^{-v(a_0)} f \in R_m$, and $\overline{\pi^{-v(a_0)} f} = \overline{\pi^{-v(a_0)} a_0} \neq 0$.

(ii) Let $\mu < m$. We then have that $v_{-m}(f) = v(a_n) - nm$. Let $B \in d\mathbb{Z}$ such that $B \geq n$. We have that $\pi^{-v(a_n)+Bm} t^{B-n} f \in R_m$, because for $k < n$ we have that

$$\begin{aligned} v(\pi^{-v(a_n)+Bm} a_k) &= -v(a_n) + Bm + v(a_k) \\ &\geq -n\mu - v(a_0) + Bm + k\mu + v(a_0) = \mu(k-n) + Bm \\ &> (B - n + k)m \end{aligned}$$

and $v(\pi^{-v(a_n)+Bm} a_n) = Bm$.

Let $B = bd$ then $\overline{\pi^{-v(a_n)+Bm} t^{B-n} f} = \overline{\pi^{-v(a_n)} a_n \pi^{dmb} t^B} = \overline{\pi^{-v(a_n)} a_n} (\overline{\pi^{dm} t^d})^b$.

(iii) Let $\mu = m$. Then $v_{-m}(f) = v(a_n) - nm = v(a_0)$. It follows that d divides n, let $n = n'd$ with $n' \in \mathbb{Z}$, so $v(a_n) - v(a_0) = n'md$. Write $a_n = a_n' \pi^{v(a_n)}$ with $a_n' \in O^\times$. For $k > 0$, we have that

$$v(\pi^{-v(a_0)} a_k) \geq k\mu = km.$$

So $\pi^{-v(a_0)} f \in R_m$, and $\overline{\pi^{-v(a_0)} f}$ has constant term $\overline{\pi^{-v(a_0)} a_0} \neq 0$ and leading term $\overline{\pi^{n'md} a_n' t^{n'd}} = \overline{a_n'} (\overline{\pi^{dm} t^d})^{n'}$.

□

Proposition 1.3.3. *The valuation ring $\mathcal{O}_{v_{-m}}$ of v_{-m} is the localization of R_m at the prime ideal P_m.*

Proof. It is clear that for polynomials $f \in K[t]$, we have $v_{-m}(f) \geq 0$ if and only if $f \in R_m$, and $v_{-m}(f) > 0$ if and only if $f \in P_m$. From this immediately follows that the localization of R_m at the prime ideal P_m is in the valuation ring $\mathcal{O}_{v_{-m}}$ of v_{-m}.

Now let $f, g \in K[t] \setminus \{0\}$ such that $v_{-m}(f/g) \geq 0$. Let $g = \gamma \prod_{i=1}^{k} g_i$ be the factorization according to the slopes of the Newton polygon of g, with $\gamma \in K^*$. Then Lemma 1.3.2 shows that there exist $a_i \in K^*$ and $b_i \in \mathbb{N}$ such that $g_i' = a_i t^{b_i} g_i \in R_m \setminus P_m$, so $v_{-m}(g_i') = 0$. Then we have that

$$\frac{f}{g} = \frac{\gamma^{-1}(\prod_i a_i t^{b_i}) f}{\prod_i g_i'}$$

with $v_{-m}(\gamma^{-1}(\prod_i a_i t^{b_i}) f) \geq 0$, so $\gamma^{-1}(\prod_i a_i t^{b_i}) f \in R_m$ and it follows that f/g is in the localization of R_m at P_m. □

Chapter 2

Hilbert's Tenth Problem

In this chapter we give an introduction to Hilbert's Tenth Problem. We start by stating Hilbert's Tenth Problem for a ring R, and give the definition of a diophantine set, together with some basic properties and examples. Then we briefly introduce the formulation of Hilbert's Tenth Problem and diophantine sets in terms of a language. After that, we turn our attention to Hilbert's Tenth Problem for rational function fields in one variable over a field K. To prove undecidability of diophantine equations over $K(t)$, Denef proved that it is enough to give a diophantine definition of the valuation ring of v_∞. This proof uses elliptic curves to build a model of the integers in $K(t)$, so we will recall some theory of elliptic curves and then give Denef's proof of this reduction theorem. We will also give the diophantine definition of the valuation ring that Denef gave for rational function fields in one variable over a real field K. To conclude, we compare Denef's definition of the valuation ring of v_∞ with other undecidability proofs for rational function fields.

2.1 Hilbert's Tenth Problem

We can formulate Hilbert's Tenth Problem for an arbitrary ring R with coefficients in R_0 (R_0 a subring of R) as follows.

Hilbert's Tenth Problem: Let R be a ring, R_0 a subring of R. Does there exist an algorithm with

input: $f \in R_0[t_1, \ldots, t_n]$ for some $n \in \mathbb{N}$,

output: "yes" if there exists $a_1, \ldots, a_n \in R$ such that $f(a_1, \ldots, a_n) = 0$ and "no" otherwise.

The reason that the ring R_0 appears in our formulation is that we have to be able to input the coefficients of our diophantine equations in a computer. So we ask that the elements of the ring R_0 can be encoded with natural numbers, such that they can be used as input, and also in a way that an algorithm can do computations with them. This concept will be formalized in part II with the definition of a recursive ring. As an example, take the field of p-adic numbers $\mathbb{Q}_p$ for some prime p. Since this field is uncountable, the p-adic numbers can not be used as input. In [Ner63], Nerode proved that diophantine equations over $\mathbb{Q}_p$ with coefficients in $\mathbb{Z}$ are decidable.

Whether diophantine equations are undecidable, also depends on the ring R_0. For example, let R be a domain of characteristic 0, it is easy to see that diophantine equations for $R[t]$ with coefficients in $\mathbb{Z}$ are decidable if and only if diophantine equations for R with coefficients in $\mathbb{Z}$ are decidable. However, in [Den78a], Denef proved that diophantine equations for $R[t]$ with coefficients in $\mathbb{Z}[t]$ are undecidable. Continuing on our example of $\mathbb{Q}_p$, it follows that diophantine equations for $\mathbb{Q}_p[t]$ with coefficients in $\mathbb{Z}$ are decidable, but diophantine equations with coefficients in $\mathbb{Z}[t]$ are undecidable.

When Hilbert formulated his Tenth Problem, a precise notion of an algorithm had not yet been developed. This changed in the 1930s, with the work of Gödel, Herbrand, Kleene, Church, Post and Turing. The formal models of computation they proposed, were all shown to be equivalent: μ-recursive functions, λ-calculus, Turing machines, ... This supports the Church-Turing thesis that states that if some method exists to carry out a calculation, then the same calculation can also be done by a Turing machine.

We will not give an exact definition of an algorithm in this thesis. Intuitively, an algorithm is a program of finite length, that takes natural numbers as input, runs

according to its finite list of instructions, and either halts and produces an output, or does not stop computing. We can think of a program that we can run on a computer, except that this computer has unlimited time and memory.

Definition 2.1.1. Let R be an integral domain. A subset $A \subseteq R^k$ is *diophantine* over R if and only if there exists an $n \in \mathbb{N}$ and a polynomial $f(a_1, \ldots, a_k, x_1, \ldots, x_n)$ with coefficients in R such that

$$A = \{(a_1, \ldots, a_k) \mid \exists x_1, \ldots, x_n \in R \text{ such that } f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0\}.$$

We can write this also as

$$(a_1, \ldots, a_k) \in A \Leftrightarrow (\exists x_1, \ldots, x_n) \quad f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0$$

and we call this a *diophantine definition* of A over R.

A relation δ on R^k is called diophantine over R if the set $\{a \in R^k \mid \delta(a)\}$ is diophantine over R.

The following proposition and its proof about unions and intersections of diophantine sets are well known.

Proposition 2.1.2. *Let R be a domain. The union of two diophantine sets is a diophantine set. Suppose the fraction field of R is not algebraically closed. Then the intersection of two diophantine sets is a diophantine set.*

Proof. Let $A, B \subseteq R^k$ be diophantine sets with defining equations respectively $f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0$ and $g(a_1, \ldots, a_k, y_1, \ldots, y_m) = 0$.

Using the vector notation $\vec{a} = (a_1, \ldots, a_k)$, we have that

$$\vec{a} \in A \cup B \Leftrightarrow (\exists \vec{x}, \vec{y}) \quad f(\vec{a}, \vec{x})g(\vec{a}, \vec{y}) = 0.$$

Since the fraction field F of R is not algebraically closed, there exists a polynomial $h = b_0 + b_1 t + \cdots + b_r t^r \in R[t]$, $r \geq 1$, with no roots in F. Let $H(u, v) = b_0 v^r + b_1 u v^{r-1} + \cdots + b_r u^r \in R[u, v]$ be the homogenization of h. Since $H(u, v) = 0$ if and only if $u = 0$ and $v = 0$, we have that

$$\vec{a} \in A \cap B \Leftrightarrow (\exists \vec{x}, \vec{y}) \quad H(f(\vec{a}, \vec{x}), g(\vec{a}, \vec{y})) = 0,$$

which completes the proof. □

The condition that the fraction field of R is not algebraically closed will hold for all the domains R over which we consider undecidability problems in this thesis.

Examples 2.1.3. We now give some examples of diophantine sets.

1. The set $\mathbb{N}$ of natural numbers is diophantine in $\mathbb{Z}$, since

$$a \in \mathbb{N} \Leftrightarrow (\exists x_1, \ldots, x_4 \in \mathbb{Z}) \quad x_1^2 + x_2^2 + x_3^2 + x_4^2 = a.$$

2. In a polynomial ring $K[t]$ over a field K, the set of constants is diophantine since the elements of K^* are the invertible elements in $K[t]$:

$$a \in K \Leftrightarrow (\exists x \in K[t]) \quad a = 0 \vee ax = 1.$$

3. An important subset of a ring R is the subset $R \setminus \{0\}$ of nonzero elements. Of course, if R is a field then the nonzero elements are exactly the invertible elements, and so R^* is diophantine. It is also well known that $\mathbb{Z} \setminus \{0\}$ is diophantine, since every nonzero integer can be written as a product of an integer coprime to 2 and an integer coprime to 3:

$$a \in \mathbb{Z} \setminus \{0\} \Leftrightarrow (\exists b, c, r, s, u, v \in \mathbb{Z}) \quad a = bc \wedge br + 2s = 1 \wedge cu + 3v = 1.$$

   This method can also be extended to prove that $K[t] \setminus \{0\}$ is diophantine in $K[t]$, with K a field. In [MB07, Theorem 3.1], Moret-Bailly proves for a large class of rings R, that $R \setminus \{0\}$ is diophantine.

2.2 Diophantine models

In the previous section we remarked that whether diophantine equations for R are undecidable also depends on the ring R_0 in which the coefficients live. In terms of logic, we can formulate this with a language. A language $\mathcal{L}$ is a set of symbols of three sorts: constants, function symbols and relation symbols. For example, the language of rings, $\mathcal{L}_R$ has two constants, 0 and 1, and two function symbols

for addition and multiplication, so $\mathcal{L}_R = \{0, 1, +, \cdot\}$. We can also enlarge $\mathcal{L}$ with symbols for extra elements of the ring. For example, in $\mathbb{Z}[t]$ we can work with the language $\{0, 1, +, \cdot, t\}$. Any language that contains $\mathcal{L}_R$ is called a *ring language*. An *$\mathcal{L}$-diophantine equation* is then an equation that can be written using variables, symbols from $\mathcal{L}$ and equality. For example, using the ring language $\mathcal{L}_R = \{0, 1, +, \cdot\}$, we can write all diophantine equations with coefficients in $\mathbb{Z}$.

So now we can consider a ring R and a language $\mathcal{L}$, and we say that Hilbert's Tenth Problem for R in the language $\mathcal{L}$ has a negative answer, if there does not exist an algorithm that decides whether $\mathcal{L}$-diophantine equations have a zero over R. Similarly, we can define an $\mathcal{L}$-diophantine set as in Definition 2.1.1, where f now has to be an $\mathcal{L}$-diophantine equation.

The results known so far of undecidability of diophantine equations for a certain ring R in a language $\mathcal{L}$, do not adapt the proof for $\mathbb{Z}$ that recursively enumerable sets are diophantine, instead they reduce to the undecidability result for $\mathbb{Z}$. This can be done by proving that $\mathbb{Z}$ is an $\mathcal{L}$-diophantine set over R, or more generally, by finding a diophantine model of the integers inside R (some undecidability proofs use a diophantine interpretation, which is a more general concept than a diophantine model, but we will not need it in this thesis).

Definition 2.2.1. Let R be a domain, $\mathcal{L}$ a ring language. A subset $\mathcal{Z} \subseteq R^k$ is an *$\mathcal{L}$-diophantine model* of $\mathbb{Z}$ if $\mathcal{Z}$ is $\mathcal{L}$-diophantine over R and if there exists a bijection $\varphi : \mathbb{Z} \to \mathcal{Z} : n \mapsto z_n$ such that the sets

$$\mathcal{Z}_+ = \{(z_n, z_m, z_{n+m}) \mid n, m \in \mathbb{Z}\}$$
$$\mathcal{Z}_\times = \{(z_n, z_m, z_{nm}) \mid n, m \in \mathbb{Z}\}$$

are $\mathcal{L}$-diophantine.

Proposition 2.2.2. *Let R be a domain, $\mathcal{L}$ a ring language. If $\mathcal{Z}$ is a an $\mathcal{L}$-diophantine model of $\mathbb{Z}$ in R, then $\mathcal{L}$-diophantine equations over R are undecidable.*

The idea of this proposition is that if $\mathcal{Z}$ is a diophantine model of $\mathbb{Z}$, then we can transfer every diophantine equation over $\mathbb{Z}$ to a diophantine equation over R. Intuitively, this can be done as follows. In a given diophantine equation over $\mathbb{Z}$, we introduce for every occurrence of a sum $a + b$ a new variable c and replace

$a + b$ by $(\exists c \in \mathcal{Z})(a, b, c) \in \mathcal{Z}_+$ (and analogously, we replace every product ab by $(\exists d \in \mathcal{Z})(a, b, d) \in \mathcal{Z}_\times$). Since $\mathcal{Z}$, $\mathcal{Z}_+$ and $\mathcal{Z}_\times$ are diophantine, this gives a diophantine equation over R. Suppose that diophantine equations over R were decidable, then we could decide whether the transferred equation has solutions in $\mathcal{Z}$, and this would imply decidability for $\mathbb{Z}$, a contradiction.

2.3 Diophantine undecidability for $K(t)$

2.3.1 Elliptic curves

Let K be a field of characteristic 0. An elliptic curve E over K is a projective curve, defined by an affine equation of the form

$$y^2 = x^3 + ax + b,$$

with $a, b \in K$ and such that $x^3 + ax + b$ has no multiple roots (this implies that the curve has no singular points). The set of K-rational points $E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathfrak{o}\}$, with $\mathfrak{o}$ the point at infinity on E, is an abelian group with identity element $\mathfrak{o}$. The affine coordinates of the sum of two points P and Q are rational functions over K in the affine coordinates of P and Q. So for every $n \in \mathbb{Z}$, the map

$$e_n : E(K) \to E(K) : P \mapsto n \cdot P := \underbrace{P + \cdots + P}_{n},$$

(where addition is meant on E), is an endomorphism of E (that is, a morphism given by rational functions in the coordinates, and that preserves the group law). If $\mathrm{End}(E) \cong \mathbb{Z}$, we say that the elliptic curve E has no complex multiplication.

Now fix an elliptic curve E over K with equation $y^2 = x^3 + ax + b$. We define the elliptic curve $\mathcal{E}$ over $K(t)$ by the equation

$$(t^3 + at + b)y^2 = x^3 + ax + b.$$

It is clear that the point $P_1 = (t, 1)$ lies on $\mathcal{E}$. For any $n \in \mathbb{Z} \setminus \{0\}$, we denote the affine coordinates of $n \cdot P_1$ with (x_n, y_n).

Each $K(t)$-rational point (u, v) on $\mathcal{E}$ induces a morphism of E (a morphism of E as a curve, so that does not have to preserve the group structure on E):

$$(u, v) : E(K) \to E(K) : (x, y) \mapsto (u(x), yv(x)).$$

The point $(t, 1)$ gives the identity morphism on E, the points (x_n, y_n) correspond to e_n. In [Den78a, Lemma 3.1] Denef proved that

$$\mathcal{E}(K(t)) \cong \mathrm{End}_K(E) \oplus E[2](K)$$

with $\mathrm{End}_K(E)$ the endomorphisms of E defined over K and $E[2](K)$ the elements of order 2 in $E(K)$ (where a point of $E(K)$ acts on E as the constant map that sends $E(K)$ to this point).

2.3.2 Denef's method

For rational function fields $K(t)$, to prove diophantine undecidability, it suffices to give a diophantine definition of the valuation ring of v_∞. With this definition, one uses elliptic curves to build a diophantine model of the integers inside $K(t)$. This method was first used by Denef ([Den78a]) in characteristic zero, to prove undecidability for $K(t)$, with K a real field. Later on, we will use the following statement of the result.

Theorem 2.3.1 ([PZ00, Theorem 2.3]). *Let K be a field and let K_0 denote the prime subfield of K. Let t be a transcendental element over K. Let $\mathcal{L}_t = \{0, 1, +, \cdot, t\}$. Suppose that there exists an $\mathcal{L}_t$-diophantine definition $\psi(x)$ such that the following hold:*

1. *for every $x \in K_0(t)$ such that $v_\infty(x) > 0$, $\psi(x)$ holds;*
2. *for every $x \in K(t)$ such that $\psi(x)$ holds, we have $v_\infty(x) > 0$.*

Then $\mathcal{L}_t$-diophantine equations over $K(t)$ are undecidable.

We now give Denef's proof of this theorem for a field K of characteristic 0.

Proof. Let E be an elliptic curve over $\mathbb{Q}$ defined by the affine equation $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Q}$, without complex multiplication, so $\mathrm{End}(E) \cong \mathbb{Z}$.

As before, we define the elliptic curve $\mathcal{E}$ over $\mathbb{Q}(t)$ by the equation

$$(t^3 + at + b)y^2 = x^3 + ax + b.$$

Denote the affine coordinates of $n(t, 1)$ with (x_n, y_n) for $n \in \mathbb{Z} \setminus \{0\}$, then $x_n, y_n \in \mathbb{Q}(t)$. Let $z_n = \frac{x_n}{ty_n}$ for $n \in \mathbb{Z} \setminus \{0\}$ and define $z_0 := 0$. We want to prove that $\mathcal{Z} = \{z_{2n} \mid n \in \mathbb{Z}\}$ is a diophantine model of $\mathbb{Z}$. Since $\mathrm{End}(E) \cong \mathbb{Z}$, we have that $2 \cdot \mathcal{E}(K(t)) \cong 2 \cdot \mathbb{Z}$, so for every point (u, v) on $\mathcal{E}(K(t))$ there exists an $n \in \mathbb{Z} \setminus \{0\}$ such that $2(u, v) = 2(x_n, y_n) = (x_{2n}, y_{2n})$. Hence

$$z \in \mathcal{Z} \Leftrightarrow (\exists x, y, u, v \in K(t))\ z = 0 \vee ((u, v) \in \mathcal{E}(K(t)) \wedge 2(u, v) = (x, y) \wedge tyz = x)$$

is an $\mathcal{L}_t$-diophantine definition of $\mathcal{Z}$ in $K(t)$.

Consider the coordinate maps $X : (x, y) \mapsto x$ and $Y : (x, y) \mapsto y$ on $\mathcal{E}$. Then for all $n \in \mathbb{Z} \setminus \{0\}$, we have that

$$z_n = \frac{x_n}{ty_n} = \frac{X(n \cdot P_1)}{\frac{X(P_1)}{Y(P_1)} Y(n \cdot P_1)} = \frac{X/Y \circ e_n}{X/Y}(P_1),$$

with $P_1 = (t, 1)$. We have that $v_\infty((\frac{X/Y \circ e_n}{X/Y})(P_1) - n) > 0$ by [Lan73, Appendix 1, Paragraph 3], therefore $v_\infty(z_n - n) > 0$ for all $n \in \mathbb{Z} \setminus \{0\}$. By definition, we also have that $v_\infty(z_0) > 0$.

So for all $n, m, k \in \mathbb{Z}$ we have that

$$v_\infty(z_{2n} - 2n + z_{2m} - 2m - z_{2k} + 2k) > 0. \tag{2.1}$$

From this follows that if $(z_{2n}, z_{2m}, z_{2k}) \in \mathcal{Z}_+$, then $n+m = k$ and $v_\infty(z_{2n}+z_{2m}-z_{2k}) > 0$. On the other hand, suppose that $v_\infty(z_{2n} + z_{2m} - z_{2k}) > 0$, then it follows from (2.1) that $v_\infty(2n + 2m - 2k) > 0$, so $2n + 2m = 2k$ or $(z_{2n}, z_{2m}, z_{2k}) \in \mathcal{Z}_+$. Since $z_{2n} + z_{2m} - z_{2k} \in \mathbb{Q}(t)$, $v_\infty(z_{2n} + z_{2m} - z_{2k}) > 0$ is by assumption equivalent with $\psi(z_{2n} + z_{2m} - z_{2k})$. Hence we showed that

$$(z_{2n}, z_{2m}, z_{2k}) \in \mathcal{Z}_+ \Leftrightarrow \psi(z_{2n} + z_{2m} - z_{2k})$$

is an $\mathcal{L}_t$-diophantine definition for $\mathcal{Z}_+$. Completely analogous, one can prove that

$$(z_{2n}, z_{2m}, z_{2k}) \in \mathcal{Z}_\times \Leftrightarrow \psi(z_{2n}z_{2m} - 2z_{2k})$$

is an $\mathcal{L}_t$-diophantine definition for $\mathcal{Z}_\times$. □

2.3.3 Diophantine definition of the valuation ring

Let K be a real field, this means that -1 is not a sum of squares in K. We now discuss the diophantine definition of the valuation ring of v_∞ that Denef gave in [Den78a].

First of all, we define a diophantine set of constants C as follows.

$$y \in C \Leftrightarrow (\exists x \in K(t)) \quad y^2 = x^3 - 4.$$

As we saw before, the equation $y^2 = x^3 - 4$ defines an elliptic curve. From Hurwitz' Theorem [Har77, Chapter IV, Corollary 2.4] follows that elliptic curves do not admit rational parametrization, so $C \subset K$. Furthermore, for every $q \in \mathbb{Q}$, there exists a $y \in \mathbb{Q}$ such that $y \in C$ and $y > q$ ([Den78a, Lemma 3.4.(iii)]).

Denef then gave the following diophantine definition of the valuation:

$$\psi(x) \Leftrightarrow (\exists a_1, \ldots, a_5, y \in K(t)) \quad y \in C \wedge (y - t)x^2 + 1 = a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2.$$

Suppose $x \in K(t)$ such that $\psi(x)$ holds and $v_\infty(x) \leq 0$. Therefore, $v_\infty((y-t)x^2+1) = 2v_\infty(x) - 1$ is negative and odd. Without loss of generality, we may suppose that $v_\infty(a_1^2) = \min_{i=1,\ldots,5}\{v_\infty(a_i^2)\}$. But then $v_\infty(a_1^2 + \cdots + a_5^2)$ is even, because otherwise we would have that $v_\infty(1 + \frac{a_2^2}{a_1^2} + \cdots + \frac{a_5^2}{a_1^2}) > 0$, and so $1 + \overline{(\frac{a_2}{a_1})}^2 + \cdots + \overline{(\frac{a_5}{a_1})}^2 = 0$, a contradiction since K is a real field.

Now suppose $x \in \mathbb{Q}(t)$ and $v_\infty(x) > 0$, then $v_\infty(tx^2) = 2v_\infty(x) - 1 > 0$. So there exists a natural number $N \in \mathbb{N}$, such that

$$|(tx^2)(r)| \leq \frac{1}{2} \qquad \text{for all } r \in \mathbb{R}, |r| > N.$$

Let $y \in \mathbb{Q}$ such that $y \in C$ and $y > N \geq 0$. Then for $|r| > N$, we have that

$$((y - t)x^2 + 1)(r) \geq -rx(r)^2 + 1 \geq \frac{1}{2} > 0,$$

and for $|r| \leq N$,

$$((y - t)x^2 + 1)(r) = (y - r)x(r)^2 + 1 \geq 1 > 0.$$

So $(y-t)x^2+1$ is a positive-definite function on $\mathbb{R}$, hence it is a sum of squares in $\mathbb{Q}(t)$. By a theorem of Pourchet in [Pou71], it follows that every sum of squares in $\mathbb{Q}(t)$, can be written as the sum of 5 squares in $\mathbb{Q}[t]$.

When we look at this diophantine definition that Denef gave of the valuation, we see that, apart from the definition of the set C, the set of $x \in K(t)$ such that $v_\infty(x) > 0$ is defined by the isotropy of a quadratic form[1] q over $K(t)$, whose coefficients depend on x. This idea plays a great role in the proof of Kim and Roush for the undecidability of $K(t)$, where K is a subfield of a nondyadic p-adic field (a finite extension of $\mathbb{Q}_p$ with p odd). Actually, they prove that the set of $x \in K(t)$ with algebraic coefficients such that $v_t(x)$ is odd, is diophantine, where K is a subfield of a p-adic field that also satisfies a certain hypothesis $\mathcal{H}$. They then adapt the method of Denef to prove diophantine undecidability for $K(t)$, with K a subfield of a p-adic field that satisfies $\mathcal{H}$. Not every subfield of a p-adic field satisfies this hypothesis, but they prove that every subfield of a p-adic field has a finite extension that satisfies $\mathcal{H}$. Since it is enough to prove diophantine undecidability for a finite extension, this then gives diophantine undecidability for $K(t)$, with K any subfield of a nondyadic p-adic field.

Below, we give their hypothesis $\mathcal{H}$, followed by their diophantine definition.

Definition 2.3.2. Let K be a subfield of a nondyadic p-adic field, let $v_\mathfrak{p}$ be a discrete valuation on K that extends the p-adic valuation on $\mathbb{Q}$. We say that K satisfies hypothesis $\mathcal{H}$ if there exists $a, b \in K$ such that the following conditions hold

1. a is a root of unity,
2. b is algebraic over $\mathbb{Q}$ and $v_\mathfrak{p}(b)$ is odd,
3. K contains a square root of -1,
4. the quadratic form $\langle 1, b\rangle\langle 1, -a\rangle$ is anisotropic over the completion $K_\mathfrak{p}$ at $v_\mathfrak{p}$,
5. the quadratic form $\langle 1, b\rangle\langle 1, -a\rangle$ is isotropic at all 2-adic completions of $\mathbb{Q}(\sqrt{-1}, a, b)$.

[1] For the definitions and notations concerning quadratic forms, we refer to Section 3.1.

Proposition 2.3.3. *Let K be a subfield of a nondyadic p-adic field and suppose that K satisfies $\mathcal{H}$ for elements $a, b \in K$. Let $U \subseteq K(t)$ a diophantine set such that $U \cap \mathbb{Q}$ is dense in $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_r}$ for every finite set $\{p_1, \ldots, p_r\}$ of prime numbers. Let $g \in K(t)$ such that $v_t(g) = 0$ or $v_t(g) = 1$ and $v_\infty(g) = -2$. Suppose that the coefficients of g are algebraic over $\mathbb{Q}$. Then $v_t(g) = 1$ if and only if there exist $c_3, c_5 \in U$ such that, with*

$$f = (1+t)^3 g(t) + c_3 t^3 + c_5 t^5,$$

both the following quadratic forms are isotropic over $K(t)$:

$$\langle 1, b\rangle\langle t, -at, -1, -f\rangle$$
$$\langle 1, b\rangle\langle t, -at, -1, -af\rangle.$$

The reader can compare this to our diophantine definition that follows from Theorem 4.1.4 and Theorem 4.1.5. We use the rational function $f(t) = g(t) + ct^2$ if $v_t(g) = 0$, with only one parameter $c \in K$, the quadratic forms are multiplied with a factor $\langle t\rangle$, and we work with 7-dimensional forms instead of 8-dimensional forms.

In part I of this thesis, we follow the line of their ideas, to prove that the valuation ring at v_∞ is diophantine for $K(t)$, with K a p-adic field (not necessarily nondyadic) or K an algebraic subfield of a p-adic field. The latter is also interesting in its own right, since we do not need to go to a finite extension that satisfies a certain hypothesis, to prove that the valuation ring is diophantine. Also, using our method in Section 3.4 with the 7-dimensional quadratic form $\langle 1, \pi\rangle\langle 1, -\gamma, -t\rangle \perp \langle f\rangle$, we can formulate our diophantine definition of the valuation ring in the way that Denef did, namely: $v_\infty(x) \geq 0$ if and only if a certain rational function f that depends on x is represented by a certain quadratic form over $K(t)$.

Kim and Roush proved in [KR92] diophantine undecidability for $\mathbb{C}(t_1, t_2)$ in the ring language $\{0, 1, +, \cdot, t_1, t_2\}$. In this article, they adapt Denef's method to work with two elliptic curves, so they use a $\mathbb{Z} \times \mathbb{Z}$-structure to prove undecidability. In the proof that a certain divisibility relation on $\mathbb{Z} \times \mathbb{Z}$ is diophantine, they use three-dimensional quadratic forms over a function field of a curve over $\mathbb{C}$.

In positive characteristic p, Pheidas gave in [Phe91] a diophantine definition of the valuation ring at t for $\mathbb{F}_q(t)$ (p odd), that does not use quadratic forms, but

rather techniques from finite fields. Videla adapted this method to characteristic 2 and so also proved undecidability for $\mathbb{F}_q(t)$ ($p = 2$) in [Vid94].

Chapter 3

Quadratic forms

In our diophantine definition of the valuation ring of v_∞ in $K(t)$, quadratic forms play a very important part. In this chapter we prove our main result concerning the isotropy of certain quadratic forms over $K(t)$, where K is a p-adic field or an algebraic subfield of a p-adic field. Namely, if $g \in K[t]$ has a particular Newton polygon, then certain quadratic forms over $K(t)$ involving g and an unknown function $s \in K(t)$ can be made isotropic.

We start with an introductory section on quadratic forms, in which we recall some definitions and well-known theorems. After that, we use the specific structure of the Witt ring (namely Springer's Theorem for complete discrete valuation fields and Milnor's exact sequence for the Witt ring of $K(t)$) to define a quadratic reciprocity symbol for polynomials over a p-adic field, and prove the usual properties that one expects of a quadratic reciprocity symbol. In the next section, we prove our main result on the isotropy of quadratic forms over a rational function field over a p-adic field. Then we consider certain rotations of isotropic vectors of the quadratic form to construct an isotropic vector with certain properties that do not depend on the prime p. And in the last section, we use these local isotropic vectors to construct an isotropic vector over the rational function field over an algebraic subfield of a p-adic field.

3.1 Introduction

In this section, we recall some basic definitions and properties of quadratic forms. For more theory of quadratic forms, in particular the Witt ring, we refer the reader to [Lam05] or [Sch85].

Let K be a field with $\operatorname{char} K \neq 2$. Let V be a finite-dimensional vector space over K and $f : V \times V \to K$ a symmetric bilinear form on V. We associate with the pair (V, f) a *quadratic form* $q : V \to K$, given by $q(v) := f(v, v)$ for $v \in V$. Since $\operatorname{char} K \neq 2$, f and q determine each other, and we call the pair (V, q) a quadratic space. Choosing a basis $e_1, \ldots, e_n$ for V, we have that

$$q(v) = q(v_1, \ldots, v_n) = \sum_{i,j} f(e_i, e_j) v_i v_j$$

with $v = \sum_{i=1}^{n} v_i e_i$. The matrix $M_f = (f(e_i, e_j))$ is called the matrix of the quadratic form. In what follows, we only consider regular quadratic forms, this means that the matrix M_f is nonsingular.

Definition 3.1.1. Let (V, q) be a quadratic space. We say that q is *isotropic* if there exists a nonzero vector $v \in V$ such that $q(v) = 0$, and v is called an *isotropic vector* of q. If $q(v) \neq 0$ for all nonzero vectors $v \in V$, q is called *anisotropic*.

Definition 3.1.2. Let (V_1, q_1) and (V_2, q_2) be quadratic spaces, we say that q_1 and q_2 are *isometric*, and denote this with $q_1 \cong q_2$, if there exists a linear isomorphism $\varphi : V_1 \to V_2$ such that $q_2(\varphi(v)) = q_1(v)$ for all $v \in V_1$.

If (V, q) is any quadratic space over K, there exist $a_1, \ldots, a_n \in K$ such that q is isometric to the quadratic form $\langle a_1, \ldots, a_n \rangle(v_1, \ldots, v_n) := a_1 v_1^2 + \cdots + a_n v_n^2$. Given two quadratic forms q_1 and q_2, one can define their (orthogonal) sum $q_1 \perp q_2$ and product $q_1 \otimes q_2$. Given a diagonal representation $q_1 \cong \langle a_1, \ldots, a_n \rangle$ and $q_2 \cong \langle b_1, \ldots, b_m \rangle$, we have that

$$\begin{aligned} q_1 \perp q_2 &\cong \langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle \\ q_1 \otimes q_2 &\cong \langle a_1 b_1, \ldots, a_1 b_m, a_2 b_1, \ldots, a_n b_m \rangle. \end{aligned}$$

The isometry class of the quadratic form $\langle 1, -1 \rangle$ is called the *hyperbolic plane*, an orthogonal sum of hyperbolic planes is called a *hyperbolic space*. Two quadratic

forms q_1 and q_2 are called *Witt equivalent*, if the orthogonal sum of q_1 and a hyperbolic space is isometric to the orthogonal sum of q_2 and a hyperbolic space. One can then form the *Witt ring* $W(K)$ of K as the ring of Witt equivalence classes of isometry classes of regular quadratic forms over K, with the given addition and multiplication. We denote the *fundamental ideal* in $W(K)$, consisting of the Witt classes of even dimension, with $I(K)$, and its powers $(I(K))^n := I^n(K)$. Mostly, we will denote the Witt equivalence class $[q]$ of a quadratic form q also with q, it will be clear from the context whether we mean isometry of quadratic forms or equality as equivalence classes in the Witt ring.

An important class of quadratic forms are Pfister forms.

Definition 3.1.3. Let $a_1, \dots, a_n \in K^*$, the quadratic form

$$\langle 1, a_1 \rangle \otimes \cdots \otimes \langle 1, a_n \rangle$$

is called an *n-fold Pfister form.*

Theorem 3.1.4 ([Lam05, Chapter X, Theorem 1.7]). *Let φ be a Pfister form over K. If φ is isotropic, then $\varphi = 0$ in the Witt ring $W(K)$.*

Now we look at a field K with a discrete valuation v. We denote the valuation ring with $\mathcal{O}$, and let π be a generator of the maximal ideal $\mathcal{M}$ in $\mathcal{O}$. Any 1-dimensional quadratic form over K can be written as $\langle u \rangle$ or $\langle \pi u \rangle$, with $u \in \mathcal{O}^\times$. Therefore, any quadratic form q of dimension n over K can be written as $q_1 \perp \langle \pi \rangle q_2$ with $q_1 = \langle u_1, \dots, u_r \rangle$ and $q_2 = \langle u_{r+1}, \dots, u_n \rangle$ where $u_i \in \mathcal{O}^\times$. Denote the reduction of an element $a \in \mathcal{O}$ modulo $\mathcal{M}$ with $\overline{a}$. Then $\overline{q_1} = \langle \overline{u_1}, \dots, \overline{u_r} \rangle$ and $\overline{q_2} = \langle \overline{u_{r+1}}, \dots, \overline{u_n} \rangle$ are called the *first* and *second residue forms of q*. We then have the *residue class maps*

$$\delta_i : W(K) \to W(\mathcal{O}/\mathcal{M}) : q \mapsto \overline{q_i}, \qquad i = 1, 2.$$

The first residue form $\overline{q_1}$ does not depend on the choice of the uniformizer π. The choice of another uniformizer $\pi' = u\pi$, $u \in \mathcal{O}^\times$, changes the second residue form $\overline{q_2}$ up to multiplying with the unit u^{-1}, but this does not affect the (an)isotropy of $\overline{q_2}$. Therefore, the residue maps δ_i are well-defined group morphisms $W(K) \to W(\mathcal{O}/\mathcal{M})$.

In the following, we will often use the following theorem by Springer to prove anisotropy of quadratic forms over a valued field.

Theorem 3.1.5 ([Sch85, Chapter 6, Corollary 2.6]). *Let K be a field with a discrete henselian valuation with residue class field k and* $\mathrm{char}(k) \neq 2$. *Then the following assertions hold:*

1. *A quadratic form q is isotropic if and only if one of the two residue class forms is isotropic.*
2. *There exists a group isomorphism $(\delta_1, \delta_2) : W(K) \to W(k) \oplus W(k)$.*
3. *Let $n \in \mathbb{N}$, $n \geq 2$. If every n-dimensional quadratic form is isotropic over k, then every $(2n-1)$-dimensional quadratic form is isotropic over K.*

In Chapter 1, we showed how every monic irreducible polynomial $p(t)$ over K determines a valuation on $K(t)$ that is trivial on K. Instead of the notation with δ_2 from before, we now denote the second residue class map with respect to this valuation with δ_p. We will use Milnor's exact sequence to prove isotropy of certain quadratic forms over $K(t)$.

Theorem 3.1.6 (Milnor exact sequence, [Lam05, Chapter IX, Theorem 3.1]). *Let i be the functorial map $W(K) \to W(K(t))$. Let $\delta = \bigoplus \delta_p$ where the direct sum extends over all monic irreducible polynomials $p(t) \in K[t]$. Then the following sequence of abelian groups is split exact*

$$0 \to W(K) \xrightarrow{i} W(K(t)) \xrightarrow{\delta} \bigoplus_p W(K[t]/(p)) \to 0.$$

We will also need the well-known Hasse-Minkowski principle for quadratic forms over number fields.

Theorem 3.1.7 (Hasse-Minkowski Principle, [Lam05, Chapter VI, Theorem 3.1]). *Let F be a number field, q a quadratic form over F. Then q is isotropic over F if and only if for every prime $\mathfrak{p}$ of F, q is isotropic over the completion $F_\mathfrak{p}$.*

3.2 A quadratic reciprocity symbol

From now on, let K be a p-adic field, that is a finite extension of some $\mathbb{Q}_p$, where p is an odd prime or $p = 2$. Fix a uniformizer π of K. We work in a fixed algebraic

closure $\bar{K}$ of K, and we normalize the valuation on K and all its finite extensions such that $v(\pi) = 1$.

The structure of the Witt ring of p-adic fields is well known, in particular we know that $I^2(K) \cong \mathbb{Z}/2\mathbb{Z}$ and that $I^3(K) = 0$ (see [Lam05, Chapter VI, Corollary 2.15]). In this section, we will define a kind of Legendre symbol for the function field $K(t)$. This symbol can be seen as the second residue map of a certain 3-fold Pfister form over $K(t)$, and takes two values in $\mu_2 = \{-1, 1\}$ according to the isotropy of this quadratic form. Since the second residue map of a quadratic form over $K(t)$ is a quadratic form over some finite extension of K, we briefly recall some theory on the behavior of quadratic forms under field extensions.

Let L/K be a field extension. Let q be a quadratic form over K. We can consider q also as a quadratic form over L, we denote this with q_L. This induces a ring morphism $i : W(K) \to W(L)$. The following theorem by Springer is well known.

Theorem 3.2.1 ([Lam05, Chapter VII, Theorem 2.7]). *Let L/K be a finite extension of odd degree. If q is an anisotropic quadratic form over K, then q_L is anisotropic over L.*

Now let L/K be a finite extension, and $s : L \to K$ a nonzero K-linear map on the K-vector space L. If q is a (regular) quadratic form over L, then $s \circ q$ is a (regular) quadratic form over K. The quadratic form $s \circ q$ is called the *transfer* of q, and is also denoted by $s_*(q)$. We have that s induces a morphism of additive groups $s_* : W(L) \to W(K)$. We recall some elementary properties of the transfer map. For more information, we refer the reader to [Sch85, Chapter 2, Section 5].

Theorem 3.2.2 ([Sch85, Chapter II, Theorem 5.6]). *Let L/K be a finite extension. If $s : L \to K$ is a nonzero K-linear map, then*

$$s_* \circ i : W(K) \to W(L) \to W(K) : q \mapsto q \otimes s_*\langle 1 \rangle.$$

Lemma 3.2.3 ([Sch85, Chapter II, Theorem 5.8]). *Let $L = K(\alpha)/K$ be a finite extension of degree n. Let $s : L \to K$ be defined by $s(1) = 1$, $s(\alpha) = \cdots = s(\alpha^{n-1}) = 0$. In $W(K)$ we have that*

$$s_*(\langle 1 \rangle) = \begin{cases} \langle 1, -N_{L/K}(\alpha) \rangle & \text{if } n \text{ is even,} \\ \langle 1 \rangle & \text{if } n \text{ is odd.} \end{cases}$$

Now we can define our quadratic reciprocity symbol.

Definition 3.2.4. Let $q(t)$ be a monic irreducible polynomial over K of degree n and let $\alpha \in \bar{K}$ be a root of q. Let $s : K(\alpha) \to K$ be defined by $s(1) = 1$, $s(\alpha) = \cdots = s(\alpha^{n-1}) = 0$. For $p(t) \in K[t]$, coprime to $q(t)$, we define a Legendre type symbol

$$\begin{aligned}\left(\frac{p}{q}\right) &= s_*\left(\delta_q\left(\langle 1,\pi\rangle\langle 1,-p(t)\rangle\langle 1,-q(t)\rangle\right)\right)\\ &= s_*\left(\langle 1,\pi\rangle\langle 1,-p(\alpha)\rangle\right) \in I^2(K) \cong \mu_2.\end{aligned}$$

The second equality is justified because $\langle -1\rangle\varphi = \varphi$ for $\varphi \in I^2(K(\alpha))$. We denote this symbol multiplicatively with values in $\mu_2 = \{-1, 1\}$, despite the fact that the operation corresponds to addition of quadratic forms in the Witt ring. This symbol is well defined for the class of $p(t) \in (K[t]/q(t))^*$.

From [Sch85, Chapter 6, Theorem 4.4] follows that $s_*(\langle 1,\pi\rangle\langle 1,-p(\alpha)\rangle)$ is zero in $W(K)$ if and only if $\langle 1,\pi\rangle\langle 1,-p(\alpha)\rangle$ is zero in $W(K(\alpha))$, as stated in the following Proposition. This means that $\left(\frac{p}{q}\right) = 1$ if and only if $\langle 1,\pi\rangle\langle 1,-p(\alpha)\rangle$ is isotropic over $K(\alpha)$. From this also follows that the value of our symbol does not depend on the choice of the map s in the definition.

Proposition 3.2.5. *Let K be a p-adic field and L a finite extension of K. Let $s : L \to K$ be a nonzero K-linear map, $s_* : W(L) \to W(K)$ the corresponding transfer map. Then s_* induces an isomorphism $I^2(L) \xrightarrow{\sim} I^2(K)$.*

Proof. Let φ be a 4-dimensional anisotropic Pfister form over L, this means that $\varphi \neq 0$ in $I^2(L)$. From [Sch85, Chapter 6, Theorem 4.4], it follows that $s_*(\varphi)$ is Witt-equivalent to the unique anisotropic 4-dimensional quadratic form over K, so $s_*(\varphi) \neq 0$ in $W(K)$ (Theorem 3.1.4). Since $I^2(L)$ and $I^2(K)$ have 2 elements, it follows that $s_* : I^2(L) \xrightarrow{\sim} I^2(K)$ is an isomorphism. □

Since $\pi\langle 1,\pi\rangle \cong \langle 1,\pi\rangle$, we have $\left(\frac{p}{q}\right) = \left(\frac{\pi^n p}{q}\right)$ for every $n \in \mathbb{Z}$. Note that the symbol clearly depends on the choice of uniformizer π. To be consistent, we will work all the time with one fixed uniformizer.

Next, we prove multiplicativity of the symbol.

Proposition 3.2.6. *Let $q(t)$ be a monic irreducible polynomial over K. Let $p(t)$ and $r(t)$ be polynomials over K, coprime to $q(t)$. Then*

$$\left(\frac{pr}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{r}{q}\right). \tag{3.1}$$

Proof. Let α be a root of q. The statement (3.1) is equivalent to

$$s_*(\langle 1,\pi\rangle\langle 1,-p(\alpha)r(\alpha)\rangle) = s_*(\langle 1,\pi\rangle\langle 1,-p(\alpha)\rangle) \perp s_*(\langle 1,\pi\rangle\langle 1,-r(\alpha)\rangle)$$

or, because of Proposition 3.2.5,

$$\langle 1,\pi\rangle\langle 1,-p(\alpha)\rangle \perp \langle 1,\pi\rangle\langle 1,-r(\alpha)\rangle \perp -\langle 1,\pi\rangle\langle 1,-p(\alpha)r(\alpha)\rangle = 0.$$

We can simplify this to

$$\begin{aligned} \langle 1,\pi\rangle\langle 1,1,-1,-p(\alpha),-r(\alpha),p(\alpha)r(\alpha)\rangle &= 0 \\ \langle 1,\pi\rangle\langle 1,-1\rangle \perp \langle 1,\pi\rangle\langle 1,-p(\alpha),-r(\alpha),p(\alpha)r(\alpha)\rangle &= 0 \\ \langle 1,\pi\rangle\langle 1,-p(\alpha)\rangle\langle 1,-r(\alpha)\rangle &= 0. \end{aligned}$$

Since 3-fold Pfister forms are hyperbolic over $K(\alpha)$, the last equality is always true. □

In the following Proposition we give the relation between the symbol $\left(\frac{c}{q}\right)$ and $\left(\frac{c}{t}\right)$ for $c \in K^*$. Remark that $\left(\frac{c}{t}\right) = 1$ if and only if $\langle 1,\pi\rangle\langle 1,-c\rangle$ is isotropic over K. So from Springer's Theorem 3.2.1 it is immediately clear that $\left(\frac{c}{q}\right) = \left(\frac{c}{t}\right)$ if q has odd degree.

Proposition 3.2.7. *Let $c \in K^*$ and $q \in K[t]$ be a monic irreducible polynomial. Then*

$$\left(\frac{c}{q}\right) = \left(\frac{c}{t}\right)^{\deg q}.$$

Proof. Let α be a root of q. Let $\varphi = \langle 1,\pi\rangle\langle 1,-c\rangle$ considered in $W(K(\alpha))$. Let $s : K(\alpha) \twoheadrightarrow K$ be defined by $s(1) = 1, s(\alpha) = \cdots = s(\alpha^{\deg(q)-1}) = 0$. By Theorem 3.2.2 we have

$$\left(\frac{c}{q}\right) = s_*(\varphi) = \langle 1,\pi\rangle\langle 1,-c\rangle s_*(\langle 1\rangle_{K(\alpha)}).$$

Since 3-fold Pfister forms are hyperbolic over K, by Lemma 3.2.3 we have

$$\left(\frac{c}{q}\right) = \begin{cases} \langle 1, \pi\rangle\langle 1, -c\rangle & \text{if } \deg q \text{ is odd} \\ 0 & \text{if } \deg q \text{ is even} \end{cases}$$

in $W(K)$. This proves the proposition. □

Next, we want to find a quadratic reciprocity law, i.e. a relation between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$. For p a monic irreducible polynomial of degree n we define the K-linear map

$$s_p : K[t]/(p) \to K$$

by $s_p(1) = s_p(t) = \ldots = s_p(t^{n-2}) = 0$, $s_p(t^{n-1}) = 1$. This map gives us the transfer homomorphism

$$(s_p)_* : W(K[t]/(p)) \to W(K).$$

For the prime at infinity, let $(s_\infty)_* = -id$. Then

Theorem 3.2.8 ([Sch85, Chapter 6, Theorem 3.5]). *Let K be a field of characteristic $\neq 2$. Let $\delta_p : W(K(t)) \to W(K[t]/(p))$ be the second residue class map with respect to the irreducible polynomial p or t^{-1} in case $p = \infty$ and let $(s_p)_*$ be the transfer homomorphism given above. For $\delta = \bigoplus \delta_p$ and $s_* = \sum (s_p)_*$ the following sequence is exact:*

$$W(K(t)) \xrightarrow{\delta} \bigoplus_{p,\infty} W(K[t]/(p)) \xrightarrow{s_*} W(K) \to 0.$$

In particular,

$$\sum_{p,\infty} (s_p)_* \delta_p(\varphi) = 0 \quad \textit{(in } W(K)\textit{)}$$

for every form $\varphi \in K(t)$.

Using this theorem, we can prove a reciprocity law for our symbol. In view of the definition of our symbol as the transfer of the second residue map of the form $\langle 1, \pi\rangle\langle 1, -p(t)\rangle\langle 1, -q(t)\rangle$, we expect the term $\delta_\infty(\langle 1, \pi\rangle\langle 1, -p(t)\rangle\langle 1, -q(t)\rangle)$ to appear in the reciprocity law.

Theorem 3.2.9. *Let $p(t)$ and $q(t)$ be monic irreducible polynomials over K. Then*

$$\left(\frac{p}{q}\right) = \left(\frac{-1}{t}\right)^{\deg p \deg q} \left(\frac{q}{p}\right). \tag{3.2}$$

Proof. Let β be a root of p and α a root of q. Consider the quadratic form $\langle 1, \pi\rangle\langle 1, -p(t)\rangle\langle 1, -q(t)\rangle$. The second residue class map applied to this form is trivial, except possibly at p, q and ∞. In those cases we have that

$$\delta_p(\langle 1, \pi\rangle\langle 1, -p(t)\rangle\langle 1, -q(t)\rangle) = -\langle 1, \pi\rangle\langle 1, -q(\beta)\rangle,$$

and

$$\delta_q(\langle 1, \pi\rangle\langle 1, -p(t)\rangle\langle 1, -q(t)\rangle) = -\langle 1, \pi\rangle\langle 1, -p(\alpha)\rangle.$$

We claim that

$$\delta_\infty(\langle 1, \pi\rangle\langle 1, -p(t)\rangle\langle 1, -q(t)\rangle) = \langle 1, \pi\rangle\langle -1, (-1)^{\deg p \deg q}\rangle.$$

Indeed, we find

$$\begin{aligned}
&\delta_\infty(\langle 1, \pi\rangle\langle 1, -p(t)\rangle\langle 1, -q(t)\rangle) = 0 = \langle 1, \pi\rangle\langle -1, 1\rangle && (\deg p \text{ even}, \deg q \text{ even}),\\
&\delta_\infty(\langle 1, \pi\rangle\langle 1, -p(t)\rangle\langle 1, -q(t)\rangle) = \langle 1, \pi\rangle\langle -1, 1\rangle && (\deg p \text{ odd}, \deg q \text{ even}),\\
&\delta_\infty(\langle 1, \pi\rangle\langle 1, -p(t)\rangle\langle 1, -q(t)\rangle) = \langle 1, \pi\rangle\langle -1, -1\rangle && (\deg p \text{ odd}, \deg q \text{ odd}).
\end{aligned}$$

From Theorem 3.2.8, it follows that

$$(s_p)_*(\langle 1, \pi\rangle\langle 1, -q(\beta)\rangle) + (s_q)_*(\langle 1, \pi\rangle\langle 1, -p(\alpha)\rangle) - \langle 1, \pi\rangle\langle -1, (-1)^{\deg p \deg q}\rangle = 0.$$

By definition and multiplicativity of the symbol, we have that

$$\langle 1, \pi\rangle\langle 1, -(-1)^{\deg p \deg q}\rangle = \left(\frac{-1}{t}\right)^{\deg p \deg q}.$$

So it follows that

$$\left(\frac{p}{q}\right) = \left(\frac{-1}{t}\right)^{\deg p \deg q}\left(\frac{q}{p}\right).$$

□

3.3 Isotropy over p-adic rational function fields

As before, K denotes a p-adic field with fixed uniformizer π. Let O denote the valuation ring of K. In this section, we prove our main theorem regarding isotropy of quadratic forms.

Main Theorem 3.3.1. *Let $\gamma \in K^*$. Let $g \in K[t]$ with $g(0) \neq 0$. If all the vertices of the Newton polygon of g have even degree, then there exists an $s \in K[t]$ such that both quadratic forms*

$$\langle 1, \pi\rangle\langle 1, -\gamma\rangle\langle 1, -s\rangle, \tag{3.3}$$
$$\langle 1, \pi\rangle\langle 1, tg\rangle\langle 1, -ts\rangle. \tag{3.4}$$

are isotropic over $K(t)$.

We will prove this theorem in two steps: we start with a given polynomial s that satisfies certain conditions, and we prove isotropy of the two forms (3.3) and (3.4), then we show that we can find a polynomial $s \in K[t]$ such that the previously given conditions hold.

Proposition 3.3.2. *Let $f, g, h \in K[t]\backslash\{0\}$. The quadratic form $\varphi = \langle 1, f\rangle\langle 1, g\rangle\langle 1, h\rangle$ is isotropic over $K(t)$ if for every monic irreducible polynomial $p \in K[t]$, the second residue form $\delta_p(\varphi)$ is isotropic.*

Proof. Suppose all the second residue maps of φ are isotropic. Since $\delta_p(\varphi)$ is a Pfister form, it follows that $\delta_p(\varphi) = 0$ in $W(K[t]/(p))$. By Theorem 3.1.6, we have that φ is in the image $i(W(K))$ of the functorial map $i : W(K) \to W(K(t))$. Therefore, φ is Witt equivalent to an anisotropic form ψ over K. Since the dimension of ψ is at most 4, it follows that φ is isotropic. □

In the following Corollary, we apply this Proposition to 3-fold Pfister forms of the form $\varphi = \langle 1, \pi\rangle\langle 1, a\rangle\langle 1, b\rangle$, with $a(t), b(t) \in K[t]$. Remark that we can always write $\varphi = \langle 1, \pi\rangle\langle 1, fh\rangle\langle 1, gh\rangle$, with $h = \gcd(a, b)$, $a = fh$ and $b = gh$, such that f, g and h are pairwise coprime. We translate the condition that the second residue forms of φ are isotropic in terms of our quadratic reciprocity symbol, since we will apply it this way in our proof of Theorem 3.3.5.

Corollary 3.3.3. *Let $f, g, h \in K[t] \setminus \{0\}$ be squarefree polynomials that are pairwise coprime. The quadratic form $\varphi = \langle 1, \pi\rangle\langle 1, fh\rangle\langle 1, gh\rangle$ is isotropic if and only*

if

$$\left(\frac{-gh}{p}\right) = 1 \quad \textit{for every irreducible factor } p \textit{ of } f,$$
$$\left(\frac{-fh}{q}\right) = 1 \quad \textit{for every irreducible factor } q \textit{ of } g,$$
$$\left(\frac{-fg}{r}\right) = 1 \quad \textit{for every irreducible factor } r \textit{ of } h.$$

Proof. From Proposition 3.3.2 follows that the quadratic form φ is isotropic if and only if all its second residue forms at prime polynomials are zero. The second residue map of the form is trivially zero, except at the irreducible factors of f, g and h. Let p be an irreducible factor of f, let $f' = f/p$. Then

$$\delta_p(\langle 1, \pi\rangle\langle 1, fh\rangle\langle 1, gh\rangle) = \langle (f'h)(\alpha)\rangle\langle 1, \pi\rangle\langle 1, g(\alpha)h(\alpha)\rangle$$

with α a root of p. By Proposition 3.2.5, this quadratic form is isotropic if and only if

$$\left(\frac{-gh}{p}\right) = 1.$$

Let q be an irreducible factor of g. Then we find analogously that the second residue form $\delta_q(\langle 1, \pi\rangle\langle 1, fh\rangle\langle 1, gh\rangle)$ is isotropic if and only if $\left(\frac{-fh}{q}\right) = 1$.

Next, let r be an irreducible factor of h and $h' = h/r$. Then

$$\delta_p(\langle 1, \pi\rangle\langle 1, fh\rangle\langle 1, gh\rangle) = \langle h'(\zeta)\rangle\langle 1, \pi\rangle\langle f(\zeta), g(\zeta)\rangle$$

with ζ a root of r. By Proposition 3.2.5, this quadratic form is isotropic if and only if

$$\left(\frac{-fg}{r}\right) = 1.$$

□

Theorem 3.3.4. *Let $\gamma \in K^*$. Let $s \in K[t]$ with $s(0) \neq 0$ and suppose that all irreducible factors of s have even degree. Then*

$$\langle 1, \pi\rangle\langle 1, -\gamma\rangle\langle 1, -s\rangle$$

is isotropic over $K(t)$.

Proof. Since each p has even degree, Proposition 3.2.7 implies that $\left(\frac{\gamma}{p}\right) = 1$ for each irreducible factor p of s. By Corollary 3.3.3 follows that $\langle 1, \pi\rangle\langle 1, -\gamma\rangle\langle 1, -s\rangle$ is isotropic over $K(t)$. □

In the following theorem, we give sufficient conditions on the factorization of $s \in K[t]$, such that the quadratic form $\langle 1, \pi\rangle\langle 1, tg\rangle\langle 1, -ts\rangle$, with a given $g \in K[t]$, is isotropic over $K(t)$. Remark that the Newton polygon of s will have the same number of edges and the same slopes as the Newton polygon of g.

Theorem 3.3.5. *Let $\gamma \in K^*$. Let $g, s \in K[t]$ with $g(0) \neq 0$ and $s(0) \neq 0$. Suppose that g and s have even degree and that g and s are squarefree. Let $g = \varepsilon \prod_{i=1}^{n} g_i$ be the factorization according to the slopes of g, let m_i be the slope of the Newton polygon of g_i, and $g_i = \prod_{j=1}^{r_i} g_{ij}$, with the g_{ij} monic and irreducible. Let $s = \varepsilon \prod_{i=1}^{n} s_i$. For each i, we let $s_i = \prod_{j=1}^{e_i} s_{ij}$, and suppose that the s_{ij} satisfy the following properties:*

(i) s_{ij} is monic irreducible with slope m_i.
(ii) s_{ij} has even degree.
(iii) s_{ij} is coprime to tg.
(iv) For all i, κ, λ with $i \neq \kappa$, the following equality holds:

$$\left(\frac{s_i}{g_{\kappa\lambda}}\right) = \left(\frac{g_i}{g_{\kappa\lambda}}\right). \tag{3.5}$$

(v) For all i, j, we have that:

$$\left(\frac{s_i}{g_{ij}}\right) = \left(\frac{tg/g_i}{g_{ij}}\right). \tag{3.6}$$

(vi) For all i, j, we have that:

$$\left(\frac{s_{ij}}{t}\right) = \prod_{\kappa,\lambda} \left(\frac{s_{ij}}{g_{\kappa\lambda}}\right). \tag{3.7}$$

Then the quadratic form

$$\langle 1, \pi\rangle\langle 1, tg\rangle\langle 1, -ts\rangle$$

is isotropic over $K(t)$.

Proof. From Corollary 3.3.3 follows that $\langle 1, \pi\rangle\langle 1, tg\rangle\langle 1, -ts\rangle$ is isotropic over $K(t)$ if and only if the following three conditions hold:

$$\left(\frac{sg}{t}\right) = 1, \tag{3.8}$$

$$\left(\frac{ts}{g_{ij}}\right) = 1 \quad \text{for all } i, j, \tag{3.9}$$

$$\left(\frac{-tg}{s_{ij}}\right) = 1 \quad \text{for all } i, j. \tag{3.10}$$

We start with checking condition (3.9). Using multiplicativity and property (3.5), we find

$$\begin{aligned}\left(\frac{ts}{g_{ij}}\right) &= \left(\frac{\varepsilon t}{g_{ij}}\right)\prod_{\mu}\left(\frac{s_\mu}{g_{ij}}\right) = \left(\frac{\varepsilon t}{g_{ij}}\right)\left(\frac{s_i}{g_{ij}}\right)\prod_{\mu\neq i}\left(\frac{g_\mu}{g_{ij}}\right)\\ &= \left(\frac{s_i}{g_{ij}}\right)\left(\frac{tg/g_i}{g_{ij}}\right) = 1,\end{aligned}$$

because of assumption (3.6).

Using the reciprocity law of our symbol in Theorem 3.2, condition (3.10) becomes

$$\left(\frac{-tg}{s_{ij}}\right) = \left(\frac{t}{s_{ij}}\right)\left(\frac{-\varepsilon}{s_{ij}}\right)\prod_{\kappa,\lambda}\left(\frac{g_{\kappa\lambda}}{s_{ij}}\right) = \left(\frac{-1}{t}\right)^{\deg s_{ij}}\left(\frac{s_{ij}}{t}\right)\left(\frac{-\varepsilon}{s_{ij}}\right)\prod_{\kappa,\lambda}\left(\frac{-1}{t}\right)^{\deg s_{ij}\deg g_{\kappa\lambda}}\left(\frac{s_{ij}}{g_{\kappa\lambda}}\right).$$

Since the degree of each s_{ij} is even, we have

$$\left(\frac{-tg}{s_{ij}}\right) = \left(\frac{s_{ij}}{t}\right)\prod_{\kappa,\lambda}\left(\frac{s_{ij}}{g_{\kappa\lambda}}\right) = 1,$$

because of assumption (3.7).

Now that conditions (3.9) and (3.10) are fulfilled, (3.8) follows automatically (be-

cause the leading coefficient of s and g is equal):

$$\begin{aligned}\left(\frac{sg}{t}\right) &= \left(\frac{\varepsilon}{t}\right)\prod_{i,j}\left(\frac{s_{ij}}{t}\right)\left(\frac{\varepsilon}{t}\right)\prod_{i,j}\left(\frac{g_{ij}}{t}\right) = \prod_{i,j}\left(\frac{-1}{t}\right)^{\deg s_{ij}}\left(\frac{t}{s_{ij}}\right)\prod_{i,j}\left(\frac{-1}{t}\right)^{\deg g_{ij}}\left(\frac{t}{g_{ij}}\right)\\ &= \left(\frac{-1}{t}\right)^{\deg s}\left(\frac{-1}{t}\right)^{\deg g}\prod_{i,j}\left(\frac{-g}{s_{ij}}\right)\prod_{i,j}\left(\frac{s}{g_{ij}}\right)\\ &= \prod_{i,j}\left[\left(\frac{-\varepsilon}{s_{ij}}\right)\prod_{\mu,\nu}\left(\frac{g_{\mu\nu}}{s_{ij}}\right)\right]\prod_{i,j}\left[\left(\frac{\varepsilon}{g_{ij}}\right)\prod_{\kappa,\lambda}\left(\frac{s_{\kappa\lambda}}{g_{ij}}\right)\right]\\ &= \prod_{i,j}\left[\left(\frac{-\varepsilon}{t}\right)^{\deg s_{ij}}\prod_{\mu,\nu}\left(\frac{-1}{t}\right)^{\deg g_{\mu\nu}\deg s_{ij}}\left(\frac{s_{ij}}{g_{\mu\nu}}\right)\right]\prod_{i,j}\left[\left(\frac{\varepsilon}{t}\right)^{\deg g_{ij}}\prod_{\kappa,\lambda}\left(\frac{s_{\kappa\lambda}}{g_{ij}}\right)\right] = 1\end{aligned}$$

since the degree of s and of g is even. □

Now we still need to find the polynomial s with the properties given in Theorem 3.3.5. To do this, we will start from a polynomial in the reduction $k[t]$, where k is the residue field of K, which we will find using the following density theorem.

Theorem 3.3.6 ([BMS67, Theorem A.10 with $S_0 = \emptyset$]). *Let F be a global field, S_∞ a finite non-empty set of primes of F, containing all archimedean primes when F is a number field. Let*

$$A = \{x \in F : v_\mathfrak{p}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S_\infty\}.$$

Suppose we are given $a, b \in A$ such that $aA + bA = A$ and for each $\mathfrak{p} \in S_\infty$ an open subgroup $V_\mathfrak{p} \subset F_\mathfrak{p}^*$ and an $x_\mathfrak{p} \in F_\mathfrak{p}^*$. Suppose also that $V_\mathfrak{p}$ has finite index in $F_\mathfrak{p}^*$ for at least one $\mathfrak{p} \in S_\infty$.

Then there exist infinitely many primes $\mathfrak{p}_0 \notin S_\infty$ such that there is a $c \in A$ satisfying

$$\begin{gathered}c \equiv a \mod b\\ c \in x_\mathfrak{p} V_\mathfrak{p} \quad \text{for all} \quad \mathfrak{p} \in S_\infty\\ cA = \mathfrak{p}_0.\end{gathered}$$

Remark that the Dirichlet density theorem on primes in arithmetic progressions follows from this Theorem by taking $F = \mathbb{Q}$, $S_\infty = \{\mathfrak{q}\}$ with $\mathfrak{q} = |\cdot|$ the usual absolute value, $A = \mathbb{Z}$, $V_\mathfrak{q} = \{r \in \mathbb{R} \mid r > 0\}$ and $x_\mathfrak{q} = 1$.

In the proof of our Main Theorem, we will also use the following Lemma.

Lemma 3.3.7. *Let R be a commutative ring and $x, y \in R$ such that $(x, y) = (1)$. Let $\rho \in R^*$ and $N \in \mathbb{N}$. Then $(x + \rho y^N, xy^N) = (1)$.*

Proof. Cubing the relation $(x, y) = (1)$, we get $(x^3, x^2y, xy^2, y^3) = (1)$. Clearly, $(x^3, x^2y, xy^2, y^3) \subseteq (x^2, y^2)$; therefore, $(x^2, y^2) = (1)$. We can continue this process by induction to get $(x^{2^n}, y^{2^n}) = (1)$ for all n, so also $(x^2, y^{2N}) = (1)$. Let $\mathcal{I} := (x + \rho y^N, xy^N)$. One can easily check that $x^2 = x(x + \rho y^N) - \rho xy^N \in \mathcal{I}$ and $y^{2N} = \rho^{-1}y^N(x + \rho y^N) - \rho^{-1}xy^N \in \mathcal{I}$. It follows that $(1) = (x^2, y^{2N}) \subseteq \mathcal{I}$, hence $\mathcal{I} = (1)$. □

We now give the proof of our Main Theorem 3.3.1.

Proof of Main Theorem. Without loss of generality, we may assume that g is a squarefree polynomial (we can divide out squared factors, this does not change the fact that all the vertices of the Newton polygon of g have even degree and this also does not change the isotropy of (3.4)). Because of the factor $\langle 1, \pi \rangle$ appearing in (3.4), multiplying g with some power of π does not change the isotropy of that quadratic form. Therefore, we may assume that the leading coefficient ε of g has valuation zero.

Let $g = \varepsilon \prod_{i=1}^{n} g_i$ be the factorization according to the slopes of g. Write $g_i = \prod_{j=1}^{r_i} g_{ij}$, where the g_{ij} are monic and irreducible. Let n_i denote the degree of g_i, let $m_i = -v(g_i(0))/n_i$ denote the slope of g_i and d_i the denominator of $m_i \in \mathbb{Q}$. Then the degree of every g_{ij} must be a multiple of d_i.

Let N be an odd integer which is a multiple of all odd d_i and large enough such that

$$N > v(4)/\min_{i \neq j} |m_i - m_j|.$$

From Theorem 3.3.4 and Theorem 3.3.5 follows that we have to find $s \in K[t]$, such that for the factorization of s according to the slopes we have that $s = \varepsilon \prod_{i=1}^{n} \prod_j s_{ij}$ with $s_i := \prod_{j=1}^{e_i} s_{ij}$, such that the s_{ij} satisfy properties (i)–(vi).

Now we will construct the s_{ij} with the desired properties. For this, we will have to distinguish two cases, according to the parity of d_i, the denominator of the slope m_i. We then define $s := \varepsilon \prod_{i=1}^{n} \prod_j s_{ij}$.

Case 1: d_i is odd.

In this case, we let $e_i = 1$, so we will construct one irreducible factor $s_i = s_{i1}$ with slope m_i. We want to construct s_i using the ring R_{m_i} (see Section 1.3). For the sake of convenience, we let $R := R_{m_i}$ and $P := P_{m_i}$. It is not hard to see that the usual Euclidean division for polynomials works in R, provided we divide by a polynomial whose leading term is not in P.

Let $u = \pi^{m_i d_i} t^{d_i}$ and $k = O/(\pi)$. Recall that $R/P = k[\overline{u}]$. For a polynomial $f(\overline{u}) \in k[\overline{u}]$, we define $\deg^\dagger f := d_i \deg f$. This is chosen such that $\deg^\dagger \overline{f} = \deg f$ for all $f \in R$ with leading term not in P.

Define $h_i := \pi^{m_i n_i} g_i$. Since g_i is monic of degree n_i and slope m_i, it follows that $h_i \in R$. By Lemma 1.3.2, we see that there exist $A, B \in \mathbb{Z}$ with B even such that $\pi^A t^B g/g_i = \varepsilon \pi^A t^B \prod_{\mu \neq i} g_\mu \in R \setminus P$. The reduction modulo P of $\pi^A t^B g/g_i$ is of the form $\rho \overline{u}^G$ with $\rho \in k^*$ and $G \geq 0$.

Since the conditions (3.6) and (3.7) do not change if we multiply s_i with a multiple of π, in reality we will construct $c := \pi^{m_i \deg s_i} s_i \in R$. We define

$$a := h_i + \pi^{m_i N + A} t^{N+B} g/g_i \in R$$
$$b := h_i u^{N/d_i + G} = \pi^{m_i(N + d_i G)} t^{N + d_i G} h_i \in R.$$

We will construct c of the form $c = a + qb$ for some $q \in R$. Using the fact that $\left(\frac{t}{g_{ij}}\right) = \left(\frac{t^{N+B}}{g_{ij}}\right)$ and $g_{ij} \mid h_i$, it is clear that $s_i := \pi^{-m_i \deg c} c = \pi^{-m_i \deg c}(a + qb)$ satisfies (3.6) and

$$\left(\frac{s_i}{t}\right) = \left(\frac{g_i}{t}\right). \tag{3.11}$$

At the same time, we will make sure that c is also of the form $r + \pi^{m_i e} t^e h_i$ for some $e \in 2d_i\mathbb{Z}$ and $r \in R$ with $\deg r \leq \deg h_i + e - N$. We claim that for such c, the following holds:

$$\left(\frac{c}{g_{\kappa\lambda}}\right) = \left(\frac{h_i}{g_{\kappa\lambda}}\right) \quad \text{for all } \kappa, \lambda \text{ with } i \neq \kappa. \tag{3.12}$$

Indeed, let α be a root of $g_{\kappa\lambda}$. If $m_i < m_\kappa = -v(\alpha)$, then by Proposition 1.2.6, the square class of $c(\alpha)$ in $K(\alpha)$ is the same as $\pi^{m_i e} h_i(\alpha)$. This implies (3.12).

If $m_i > m_\kappa$, then the square class of $c(\alpha)$ in $K(\alpha)$ is the same as $a(\alpha)$. Since $(g/g_i)(\alpha) = 0$, this also implies (3.12). Using $\left(\frac{s_i}{g_{\kappa\lambda}}\right) = \left(\frac{c}{g_{\kappa\lambda}}\right)$ and $h_i = \pi^{m_i n_i} g_i$, it is clear that (3.12) implies (3.5).

Using (3.5) and (3.6), we can rewrite the right hand side of condition (3.7) as

$$\begin{aligned}
\prod_{\kappa,\lambda}\left(\frac{s_i}{g_{\kappa\lambda}}\right) &= \prod_{\kappa\neq i,\lambda}\left(\frac{s_i}{g_{\kappa\lambda}}\right)\prod_j\left(\frac{s_i}{g_{ij}}\right) = \prod_{\kappa\neq i,\lambda,j}\left(\frac{g_{ij}}{g_{\kappa\lambda}}\right)\prod_j\left(\frac{tg/g_i}{g_{ij}}\right)\\
&= \prod_{\kappa\neq i,\lambda,j}\left(\frac{-1}{t}\right)^{\deg g_{\kappa\lambda}\deg g_{ij}}\left(\frac{g_{\kappa\lambda}}{g_{ij}}\right)\prod_j\left(\frac{tg/g_i}{g_{ij}}\right)\\
&= \prod_{\kappa\neq i}\left(\frac{-1}{t}\right)^{\deg g_\kappa \deg g_i}\prod_j\left(\frac{\varepsilon^{-1}g/g_i}{g_{ij}}\right)\prod_j\left(\frac{tg/g_i}{g_{ij}}\right)\\
&= \prod_j\left(\frac{\varepsilon^{-1}t}{g_{ij}}\right) = \prod_j\left(\frac{\varepsilon^{-1}}{t}\right)^{\deg g_{ij}}\left(\frac{-1}{t}\right)^{\deg g_{ij}}\left(\frac{g_{ij}}{t}\right) = \left(\frac{g_i}{t}\right).
\end{aligned}$$

Because of (3.11), condition (3.7) will also be satisfied now that we construct s_i in the required form.

The ideal $P + (u)$ in R contains all $\pi^\alpha t^\beta \in R$, except for $\pi^0 t^0$. The constant term of h_i has valuation zero, therefore $(h_i) + P + (u) = (1)$. Note that $\overline{a} = \overline{h_i} + \rho\overline{u}^{N/d_i+G}$ and $\overline{b} = \overline{h_i}\overline{u}^{N/d_i+G}$. Since $(\overline{h_i}, \overline{u}) = (1)$ in R/P, Lemma 3.3.7 implies $(\overline{a}, \overline{b}) = (1)$.

Let $N' := N/d_i$. We apply Theorem 3.3.6 to $k = R/(P+(u))$, $F = k(\overline{u})$, $S_\infty = \{\mathfrak{p}_\infty\}$, then $A = k[\overline{u}]$. Take

$$\begin{aligned}
V_\infty &= \{\overline{u}^{e'} + c_{e'-N'}\overline{u}^{e'-N'} + c_{e'-N'-1}\overline{u}^{e'-N'-1} + \cdots + c_0 + c_{-1}\overline{u}^{-1} + \cdots \mid e' \in 2\mathbb{Z}\}\\
&\subseteq k((\overline{u}^{-1})) = k_\infty
\end{aligned}$$

and $x_\infty = \overline{h_i}$. Because of Theorem 3.3.6, there exist infinitely many $\overline{q_1} \in k[\overline{u}]$ such that $\overline{c} := \overline{a} + \overline{q_1}\overline{b} \in k[\overline{u}]$ is irreducible and in $\overline{h_i}V_\infty$. There are infinitely many, so we may assume that $\deg^\dagger \overline{c} \geq N + \deg b$.

Since $\overline{c} \in \overline{h_i}V_\infty$, we can write $\overline{c} = \overline{h_i}(\overline{u}^{e'} + \overline{r_0})$, with $\overline{r_0} \in k((\overline{u}^{-1}))$ such that $\deg \overline{r_0} \leq e' - N'$. Let $\overline{r_1} = \overline{h_i}\overline{r_0} = \overline{c} - \overline{h_i}\overline{u}^{e'} \in k[\overline{u}]$, then $\deg^\dagger \overline{r_1} \leq n_i + e - N$. Choose a lift $r_1 \in R$ of $\overline{r_1}$ such that $\deg r_1 = \deg^\dagger \overline{r_1}$. Now let $\tilde{c} = r_1 + \pi^{m_i e}t^e h_i \in R$, then $\tilde{c}$ is a lift of $\overline{c}$.

Let $q_1 \in R$ be a lift of $\overline{q_1}$. Lifting the equality $\overline{c} = \overline{a} + \overline{q_1}\overline{b}$ to R yields an error term which is in P, so there exists an $f \in P$ such that

$$\tilde{c} + f = a + q_1 b. \tag{3.13}$$

Since the leading term of b is not in P, we can do Euclidean division of f by b: let $f = q_2 b + r_2$ with $\deg r_2 < \deg b$. Plugging this into (3.13) gives $\tilde{c} + r_2 = a + (q_1 - q_2)b$.

Reducing the equality $f = q_2 b + r_2$ modulo P gives $0 = \overline{q_2}\overline{b} + \overline{r_2}$. The leading term of b does not vanish modulo P, so $\deg^\dagger \overline{r_2} \leq \deg r_2 < \deg b = \deg^\dagger \overline{b}$. Since $\overline{r_2}$ is a multiple of $\overline{b}$, it follows that $\overline{r_2} = 0$.

Define $c := \tilde{c} + r_2$, $q := q_1 - q_2$ and $r := r_1 + r_2$. Then

$$c = a + qb = r + \pi^{m_i e} t^e h_i,$$

which is of the required form. It remains to check that c is irreducible. Suppose c is reducible in $K[t]$, so $c = c_1 c_2$ with $c_1, c_2 \in K[t]$. Without loss of generality we can assume that $c_1(0) = 1$. Since $c_2(0) = c(0) = h_i(0)$ is a unit and c_1 and c_2 have slope m_i, it follows that $c_1, c_2 \in R$. Therefore, we can reduce modulo P to find $\overline{c} = \overline{c_1}\,\overline{c_2}$. Now the irreducibility of $\overline{c}$ together with $\deg^\dagger \overline{c} = \deg c$ implies that c is irreducible.

Case 2: d_i is even.

In this case, every g_{ij} has even degree. The previous method will not work because every odd degree monomial in R_{m_i} becomes zero in R_{m_i}/P_{m_i}. Instead we will construct for each monic irreducible factor g_{ij} of g_i an irreducible s_{ij}. We let

$$s_{ij} := g_{ij} + p_{ij}$$

with $p_{ij} \in R_{m_i}$, such that $p_{ij} \equiv \pi^A t g / g_{ij} \pmod{g_{ij}}$ with $\deg p_{ij} < \deg g_{ij}$ for an $A \in \mathbb{N}$. By [Ser80, Chapter II, Section 2, Exercise 2], s_{ij} will be irreducible if the valuation of the coefficients of p_{ij} is sufficiently large (depending on g_{ij}). This can be done by choosing A large enough.

Next, we want to check that

$$\left(\frac{g_{ij} + p_{ij}}{g_{\mu\nu}}\right) = \left(\frac{g_{ij}}{g_{\mu\nu}}\right) \qquad \text{for all } (\mu, \nu) \neq (i, j). \tag{3.14}$$

Since $g_{ij}(\alpha) \neq 0$ for each root α of $g_{\mu\nu}$ with $(\mu,\nu) \neq (i,j)$ and for $\alpha = 0$, we can make sure that $v(p_{ij}(\alpha)) > v(g_{ij}(\alpha)) + v(4)$ for each root α of $g_{\mu\nu}$ with $(\mu,\nu) \neq (i,j)$ and for $\alpha = 0$ by taking the coefficients of p_{ij} to have large enough valuation. Let $f(x) = x^2 - (1 + g_{ij}(\alpha)^{-1} p_{ij}(\alpha))$, then

$$v(f(1)) = v(p_{ij}(\alpha)) - v(g_{ij}(\alpha)) > v(4) = 2v(f'(1)).$$

From Hensel's Lemma 1.1.2 follows that $1 + g_{ij}(\alpha)^{-1} p_{ij}(\alpha)$ is a square, so $g_{ij}(\alpha)$ and $(g_{ij} + p_{ij})(\alpha)$ are in the same square class. Therefore (3.14) is satisfied, which clearly implies (3.5), and we also have that

$$\left(\frac{s_{ij}}{t}\right) = \left(\frac{g_{ij}}{t}\right). \tag{3.15}$$

Using (3.14), we rewrite condition (3.6):

$$\begin{aligned} \prod_{\nu} \left(\frac{s_{i\nu}}{g_{ij}}\right) &= \left(\frac{tg/g_i}{g_{ij}}\right) \\ \left(\frac{s_{ij}}{g_{ij}}\right) \prod_{\nu \neq j} \left(\frac{g_{i\nu}}{g_{ij}}\right) &= \left(\frac{tg/g_i}{g_{ij}}\right) \\ \left(\frac{p_{ij}}{g_{ij}}\right) &= \left(\frac{tg/g_{ij}}{g_{ij}}\right) \end{aligned}$$

This condition is satisfied since we chose p_{ij} such that $p_{ij} \equiv \pi^A tg/g_{ij} \pmod{g_{ij}}$. Using the fact that g_{ij} has even degree, the right hand side of (3.7) becomes

$$\begin{aligned} \prod_{\kappa,\lambda} \left(\frac{s_{ij}}{g_{\kappa\lambda}}\right) &= \left(\frac{s_{ij}}{g_{ij}}\right) \prod_{(\kappa,\lambda)\neq(i,j)} \left(\frac{g_{ij}}{g_{\kappa\lambda}}\right) = \left(\frac{p_{ij}}{g_{ij}}\right) \prod_{(\kappa,\lambda)\neq(i,j)} \left(\frac{g_{\kappa\lambda}}{g_{ij}}\right) \\ &= \left(\frac{tg/g_{ij}}{g_{ij}}\right)\left(\frac{\varepsilon^{-1} g/g_{ij}}{g_{ij}}\right) = \left(\frac{\varepsilon^{-1}}{g_{ij}}\right)\left(\frac{t}{g_{ij}}\right) = \left(\frac{g_{ij}}{t}\right). \end{aligned}$$

and because of (3.15), this implies that condition (3.7) is satisfied. □

Our Main Theorem easily implies the following corollary. If the residue characteristic of K is odd, the corollary corresponds to [KR95, Theorem 17].

Corollary 3.3.8. *Let K be a p-adic field with uniformizer π and let $\gamma \in K^*$. Let $g \in K[t]$ with $g(0) \neq 0$. If all the vertices of the Newton polygon of g have even degree, then the quadratic form*

$$\langle 1, \pi \rangle \langle 1, -\gamma, -t \rangle \perp \langle -g \rangle$$

is isotropic over $K(t)$.

Proof. It follows from Theorem 3.3.1 that there exists an $s \in K[t]$ such that the quadratic forms (3.3) and (3.4) are isotropic. By Theorem 3.1.4, these forms are zero in the Witt ring.

Therefore, in $W(K(t))$ we also have

$$\begin{aligned} 0 &= \langle 1, \pi \rangle \langle 1, -\gamma \rangle \langle 1, -s \rangle \perp \langle -t \rangle \langle 1, \pi \rangle \langle 1, tg \rangle \langle 1, -ts \rangle \\ 0 &= \langle 1, \pi \rangle \langle 1, -\gamma, -s, \gamma s, -t, -g, s, -tgs \rangle \\ 0 &= (\langle 1, \pi \rangle \langle 1, -\gamma, -t \rangle \perp \langle -g \rangle) \perp (\langle s \rangle \langle 1, \pi \rangle \langle -1, \gamma, 1, -tg \rangle \perp \langle -\pi g \rangle) \,. \end{aligned}$$

This implies

$$\langle 1, \pi \rangle \langle 1, -\gamma, -t \rangle \perp \langle -g \rangle = -\langle s \rangle \langle 1, \pi \rangle \langle \gamma, -tg \rangle \perp \langle \pi g \rangle \quad \text{in } W(K(t)).$$

Since the right hand side has dimension 5 and the left hand side dimension 7, it follows that the left hand side is isotropic. □

3.4 Rotations

In Corollary 3.3.8, we proved isotropy over $K(t)$ (with K a p-adic field) of the form

$$q = \langle 1, \pi \rangle \langle 1, -\gamma, -t \rangle \perp \langle -g \rangle$$

under the condition that all the vertices of the Newton polygon of g have even degree, but we need to know more about the isotropic vectors of q. In this section, we prove in Theorem 3.4.5 that we can find an isotropic vector of q that satisfies certain properties independent of π. To do this, we transform an isotropic vector

of q in $K[t]$, using certain isometries of q, namely rotations. This was also done by Kim and Roush in [KR95], but in their article it is not always clear which rotation they perform and that the properties the isotropic vector already satisfies, are preserved under rotation, all of which is now explicitly done in our proof. One of the other differences is that we work with the 7-dimensional quadratic form $q = \langle 1, \pi\rangle\langle 1, -\gamma, -t\rangle \perp \langle -g\rangle$, instead of their 8-dimensional quadratic form $q' = \langle 1, \pi\rangle\langle 1, -\gamma, -t, -g\rangle$.

Let $\langle c_1, \ldots, c_n\rangle$ be a quadratic form of dimension n over $K(t)$ (K a field of characteristic 0). Without loss of generality, we can assume that $c_i \in K[t]$ for all $i = 1, \ldots, n$. In the following, we consider isometries of $\langle c_1, \ldots, c_n\rangle$ with determinant 1, on a 2-dimensional subspace (also called rotations). For the subspace $\langle c_i, c_j\rangle$, one can prove that the matrix of such a rotation is of the form

$$\begin{pmatrix} \dfrac{1 - c_i c_j a^2}{1 + c_i c_j a^2} & \dfrac{2ac_j}{1 + c_i c_j a^2} \\[2ex] \dfrac{-2ac_i}{1 + c_i c_j a^2} & \dfrac{1 - c_i c_j a^2}{1 + c_i c_j a^2} \end{pmatrix},$$

with $a \in K(t)$. We then have that such a rotation, followed by a rescaling with $(1 + c_i c_j a^2)$, transforms a vector $(x_1, \ldots, x_n)$ into the vector $(y_1, \ldots, y_n)$ with

$$y_i = (1 - c_i c_j a^2)x_i + 2ac_j x_j \tag{3.16}$$

$$y_j = -2ac_i x_i + (1 - c_i c_j a^2)x_j \tag{3.17}$$

$$y_k = (1 + c_i c_j a^2)x_k \qquad \text{for all } k \neq i, j. \tag{3.18}$$

In the following, we will call this rotation on a 2-dimensional subspace, followed by a rescaling, simply the rotation $\rho_{i,j}$, where a is interpreted as a polynomial variable.

Remark 3.4.1. Let R be a UFD, $f, g \in R[a]$ nonzero polynomials. We denote the resultant of f and g with $\mathrm{Res}_a(f, g)$ and the discriminant of f with $\Delta_a(f)$. If $\deg f = n$ and f_n is the leading coefficient of f, we have that $\mathrm{Res}_a(f, f') = (-1)^{n(n-1)/2} f_n \Delta_a(f)$ (with f' the formal derivative of f).

Let R be a UFD. Although the gcd of elements $a, b \in R \setminus \{0\}$ is only determined up to a unit, we will denote any gcd of a and b with $\gcd(a, b)$. With the notation "$\gcd(a, b) = \gcd(a', b')$", we mean that $\gcd(a, b)$ and $\gcd(a', b')$ are associated.

Remark 3.4.2. Let R be a UFD, $f \in R[a]$ a nonzero polynomial. We denote the content of f, that is, the gcd of the coefficients of f, with $\mathrm{cont}_a(f) \in R$.

Lemma 3.4.3. *Let R be a UFD with* $\operatorname{char} R = 0$*, $q = \langle c_1, \ldots, c_n \rangle$ a quadratic form over the fraction field of R with $c_1, \ldots, c_n \in R \setminus \{0\}$. Let $x_1, \ldots, x_n \in R$.*

1. *Suppose $x_i \neq 0$ or $x_j \neq 0$. After the rotation $\rho_{i,j}$, $y_i \neq 0$ and $y_j \neq 0$ in $R[a]$.*
2. *Let $k, l \in \{1, \ldots, n\}$, $k \neq l$. Let $p \in R$ be an irreducible element, suppose that $p \nmid x_i$. After the rotation $\rho_{k,l}$, $p \nmid y_i \in R[a]$.*
3. *Let $i, j \in \{1, \ldots, n\}$, $i \neq j$ be such that $c_i x_i^2 + c_j x_j^2 \neq 0$. After the rotation $\rho_{i,j}$,*
$$\gcd_{R[a]}(y_1, \ldots, y_n) = \gcd_R(x_1, \ldots, x_n).$$

Proof.

1. From the equations (3.16) and (3.17) follows that if x_i and x_j are not both zero, then $y_i \neq 0$ and $y_j \neq 0$ in $R[a]$.
2. Suppose $p \nmid x_i$ and perform the rotation $\rho_{k,l}$. From the equations (3.16), (3.17) and (3.18), we see that the coefficient of the constant term of $y_i \in R[a]$ is x_i, hence $p \nmid y_i$.
3. With the equations (3.16) and (3.17), one can compute
$$\mathrm{Res}_a(y_i, y_j) = -4c_i c_j (c_i x_i^2 + c_j x_j^2)^2.$$
Since this is nonzero by assumption, $\gcd_{R[a]}(y_i, y_j) \in R \setminus \{0\}$. Let $d := \gcd_{R[a]}(y_i, y_j)$. We have that d divides the content of y_i and y_j (as polynomials in a), so $d \mid \gcd_R(x_i, x_j)$. On the other hand, from equations (3.16) and (3.17) follows that $\gcd_R(x_i, x_j)$ divides y_i and y_j, so
$$\gcd_R(x_i, x_j) = \gcd_{R[a]}(y_i, y_j). \tag{3.19}$$

From equation (3.18) follows that

$$\begin{aligned}\gcd_{R[a]}(\{y_k \mid k \neq i, j\}) &= \gcd_R(\{(1 + c_i c_j a^2)x_k \mid k \neq i, j\}) \\ &= (1 + c_i c_j a^2)\gcd_R(\{x_k \mid k \neq i, j\}). \qquad (3.20)\end{aligned}$$

Since $x_i \neq 0$ or $x_j \neq 0$, we have that $\gcd_R(x_i, x_j) \in R \setminus \{0\}$. Furthermore, we have that $(1 + c_i c_j a^2) \nmid \gcd_R(x_i, x_j)$, so it follows from (3.19) and (3.20) that $\gcd_{R[a]}(y_1, \ldots, y_n) = \gcd_R(x_1, \ldots, x_n)$.

□

Lemma 3.4.4. *Let R be a UFD with $\operatorname{char} R = 0$, $s \in R[a]$ a nonzero polynomial. Suppose that $\Delta_a(s) \neq 0$. Then for all $r \in R[a]$ such that $r^2 \mid s$, we have that $r^2 \mid \operatorname{cont}_a(s)$.*

Proof. Let $r \in R[a]$ such that $r^2 \mid s$, then $r \mid \gcd(s, s')$. Since $\Delta_a(s) \neq 0$, we have that $\operatorname{Res}_a(s, s') \neq 0$, hence $\gcd(s, s') \in R \setminus \{0\}$. Therefore, $r \in R \setminus \{0\}$ so $r^2 \mid \operatorname{cont}_a(s)$. □

In the following Theorem, we carry out the rotations on isotropic vectors of the quadratic form $\langle 1, \pi\rangle\langle 1, -\gamma, -t\rangle \perp \langle -g\rangle$ to get an isotropic vector with certain properties. This corresponds to [KR95, Proposition 19] when the residue characteristic is odd.

Theorem 3.4.5. *Let K be a p-adic field with uniformizer π and let $\gamma \in K^*$ such that the form $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over K. Let $g \in K[t]$ be a squarefree nonconstant polynomial with $g(0) \neq 0$ and all the vertices of the Newton polygon of g have even degree. Let $(x_1, \ldots, x_7)$, $x_i \in K[t]$, be an isotropic vector of $q = \langle 1, \pi\rangle\langle 1, -\gamma, -t\rangle \perp \langle -g\rangle$ and $s := x_1^2 + \pi x_2^2 - \gamma x_3^2 - \pi\gamma x_4^2$. Then for every $M \in \mathbb{N}$ such that $2M \geq \deg s + 20$, q has an isotropic vector $(y_1, \ldots, y_7)$ with $y_i \in K[t]$ such that the following hold:*

1. *$S := y_1^2 + \pi y_2^2 - \gamma y_3^2 - \pi\gamma y_4^2$ is squarefree,*
2. *$\deg S = 2M$.*

Proof. We divide out all common factors occurring in the vector $(x_1, \ldots, x_7)$, so that $\gcd_{K[t]}(x_1, \ldots, x_7) = 1$. We will perform r rotations on this isotropic vector with parameter a_i, and get a resulting isotropic vector with components in $K[t, a_1, \ldots, a_r]$. After the ℓ-th rotation, we will denote the resulting isotropic vector with $((x_\ell)_1, \ldots, (x_\ell)_7)$ and $s_\ell = (x_\ell)_1^2 + \pi(x_\ell)_2^2 - \gamma(x_\ell)_3^2 - \pi\gamma(x_\ell)_4^2$ without explicitly writing the extra variable a_i, to keep notations from becoming too heavy. We also use the notation $R_i := K[a_1, \ldots, a_i]$ for $i = 1, \ldots, r$. For practical reasons, we will sometimes write $q = \langle c_1, \ldots, c_7 \rangle$, with $c_1 = 1, c_2 = \pi, c_3 = -\gamma, c_4 = -\gamma\pi, c_5 = -t, c_6 = -\pi t$ and $c_7 = -g$.

Since $\langle 1, \pi \rangle \langle 1, -\gamma \rangle$ is anisotropic over K, we have that $\langle 1, \pi \rangle \langle 1, -\gamma \rangle$ is anisotropic over $K(t)$. Suppose that $x_i = 0$ for all $i \in \{1, 2, 3, 4\}$. Since for at least one $k \in \{1, \ldots, 7\}$ we have that $x_k \neq 0$, (x_5, x_6, x_7) is an isotropic vector of the quadratic form $\langle t, \pi t, g \rangle$. However, by taking residue maps at t, from Theorem 3.1.5 follows that $\langle t, \pi t, g \rangle$ is anisotropic over $K(t)$. So for at least one $j \in \{1, 2, 3, 4\}$, we have that $x_j \neq 0$. Furthermore $\deg s = \max(\deg(x_1^2), \ldots, \deg(x_4^2))$, again since $\langle 1, \pi \rangle \langle 1, -\gamma \rangle$ is anisotropic over K.

In the following, we fix $j_0 \in \{1, 2, 3, 4\}$ such that $x_{j_0} \neq 0$. By taking residue maps at t, from Theorem 3.1.5 follows that the quadratic form $\langle 1, \pi \rangle \langle 1, -\gamma, -t \rangle$ is anisotropic over $K(t)$. So $x_7 \neq 0$, and $c_{j_0} x_{j_0}^2 + c_k x_k^2 \neq 0$ for every $k \in \{1, \ldots, 6\}$, $k \neq j_0$.

From Lemma 3.4.3.1 follows that with the 5 rotations $\rho_{j_0,k}$, with $k \neq j_0$, $k \neq 7$, we can make an isotropic vector $((x_5)_1, \ldots, (x_5)_7)$, such that $(x_5)_i \neq 0$ for every $i \in \{1, \ldots, 7\}$. Since $c_{j_0}(x_\ell)_{j_0}^2 + c_k(x_\ell)_k^2 \neq 0$ for every $k \in \{1, \ldots, 6\}$, $k \neq j_0$ and every $\ell \in \{0, \ldots, 4\}$, we have from Lemma 3.4.3.3 that after these rotations, $\gcd_{R_5[t]}((x_5)_1, \ldots, (x_5)_7) = 1$ ($R_5 := K[a_1, \ldots, a_5]$). Looking at the equations (3.16), (3.17), (3.18), we see that $\deg_t s_5 = \deg_t s + 4$, since the degree only goes up with the rotations $\rho_{j_0,5}$ and $\rho_{j_0,6}$. Furthermore, after each of the rotations that will follow in the rest of the proof, from Lemma 3.4.3.1 follows that we will still have $(x_\ell)_i \neq 0$ for all $i = 1, \ldots, 7$, $\ell = 5, \ldots, r$.

The next step is to make s_r squarefree. To do this, we will perform the 8 rotations $\rho_{i,j}$ with $i \in \{1, 2, 3, 4\}$ and $j \in \{5, 6\}$. Let $\ell \in \{5, \ldots, 12\}$. After the $(\ell + 1)$-th

rotation we have that

$$s_{\ell+1} = \left(s_\ell - c_i(x_\ell)_i^2\right)(1 + c_i c_j a_{\ell+1}^2)^2 + c_i\left((x_\ell)_i(1 - c_i c_j a_{\ell+1}^2) + 2a_{\ell+1}c_j(x_\ell)_j\right)^2 \tag{3.21}$$

$$= c_i^2 c_j^2 s_\ell a_{\ell+1}^4 - 4c_i^2 c_j^2 (x_\ell)_i (x_\ell)_j a_{\ell+1}^3 + c_i c_j\left(-4c_i(x_\ell)_i^2 + 4c_j(x_\ell)_j^2 + 2s_\ell\right) a_{\ell+1}^2 + 4c_i c_j (x_\ell)_i (x_\ell)_j a_{\ell+1} + s_\ell. \tag{3.22}$$

Next we show that $\Delta_{a_{\ell+1}}(s_{\ell+1}) \neq 0$. One can check that

$$\Delta_{a_{\ell+1}}(s_{\ell+1}) = 4096 c_i^6 c_j^6 (s_\ell - c_i(x_\ell)_i^2)^2 (s_\ell + c_j(x_\ell)_j^2)^2 (c_i(x_\ell)_i^2 + c_j(x_\ell)_j^2)^2.$$

It is clear that $c_i \neq 0$ and $c_j \neq 0$. Furthermore, since all variables are different from zero and the quadratic forms $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ and $\langle t, \pi t, g\rangle$ are anisotropic over $K(t)$, we have that $s_\ell - c_i(x_\ell)_i^2 \neq 0$ and $s_\ell + c_j(x_\ell)_j^2 \neq 0$. By consideration of the degrees in t, we also have that $c_i(x_\ell)_i^2 + c_j(x_\ell)_j^2 \neq 0$.

Suppose that s_{13} is not squarefree. Let $p \in R_{13}[t]$ be an irreducible element such that $p^2 \mid s_{13}$. Since $\Delta_{a_{13}}(s_{13}) \neq 0$, from Lemma 3.4.4 follows that $p^2 \mid \mathrm{cont}_{a_{13}}(s_{13})$. Since $\mathrm{cont}_{a_{\ell+1}}(s_{\ell+1}) \mid s_\ell$, it follows that $p^2 \mid s_{12}$. Continuing this way, we have that $p^2 \mid \mathrm{cont}_{a_{\ell+1}}(s_{\ell+1})$ for all $\ell \in \{5, \ldots, 12\}$, so $p^2 \mid s_\ell$ for all $\ell \in \{5, \ldots, 13\}$.

We have that $p \neq t$, since $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over K.

Since $\gcd_{R_5[t]}((x_5)_1, \ldots, (x_5)_7) = 1$, it is clear that there exists a $k \in \{1, \ldots, 7\}$ such that $p \nmid (x_5)_k$. Suppose that $p \nmid (x_5)_7$ and $p \mid (x_5)_1, \ldots, (x_5)_6$. From $\sum_{i=1}^7 c_i(x_5)_i^2 = 0$ follows that $p^2 \mid c_7(x_5)_7^2$, and since $c_7 = g$ is squarefree, we have that $p \mid (x_5)_7$, a contradiction. So there exists $i \in \{1, 2, 3, 4\}$ and $j \in \{5, 6\}$ (depending on p) such that $p \nmid (x_5)_i$ or $p \nmid (x_5)_j$. From Lemma 3.4.3.2 follows that

$$p \nmid (x_\ell)_i \quad \text{or} \quad p \nmid (x_\ell)_j, \tag{3.23}$$

for every $\ell \in \{5, \ldots, 13\}$. Since $c_i \in K$ and $c_j \mid t$, we also know that

$$p \nmid c_i \quad \text{and} \quad p \nmid c_j. \tag{3.24}$$

We have that $\rho_{i,j}$ is the $(\ell + 1)$-th rotation for some $\ell \in \{5, \ldots, 12\}$. Since $p^2 \mid \mathrm{cont}_{a_{\ell+1}}(s_{\ell+1})$, by considering the coefficients of $a_{\ell+1}^0$, $a_{\ell+1}^1$ and $a_{\ell+1}^2$ in (3.22) follows

that

$$\begin{aligned} &p^2 \mid s_\ell, \\ &p^2 \mid (x_\ell)_i (x_\ell)_j, \\ &p^2 \mid -c_i (x_\ell)_i^2 + c_j (x_\ell)_j^2. \end{aligned} \tag{3.25}$$

Since $p^2 \mid (x_\ell)_i (x_\ell)_j$, we can assume without loss of generality that $p \mid (x_\ell)_i$. By (3.25) follows that also $p \mid (x_\ell)_j$. This is a contradiction with (3.23), so s_{13} is squarefree.

We have executed all 8 rotations $\rho_{i,j}$ with $i \in \{1,2,3,4\}$ and $j \in \{5,6\}$. From the equations (3.16), (3.17), (3.18) follows that the degree of s_ℓ in t increases after every rotation with $2 \deg c_j$. So after these 8 rotations, we have that $\deg s_{13} = \deg s_5 + 16 = \deg s + 20$.

Now, take $M \in \mathbb{N}$ such that $2M \geq \deg_t s_{13}$, we have to find an isotropic vector such that $\deg_t s_r = 2M$. We will now show that we can increase the degree of s_{13} in t with $2N = 2M - \deg_t s_{13}$. Perform N rotations $\rho_{1,5}$, from equation (3.22) follows that every rotation increases the degree of s_{13} in t with 2. By the same reasoning as before, we find an isotropic vector $((x_{13+N})_1, \ldots, (x_{13+N})_7)$ such that $\gcd_{R_{13+N}[t]}((x_{13+N})_1, \ldots, (x_{13+N})_7) = 1$ and $s_{13+N} \in R_{13+N}[t]$ is squarefree.

Let $r = 13 + N$. After the r rotations that we executed above, we have an isotropic vector with components $(x_r)_i \in K[t, a_1, \ldots, a_r] \setminus \{0\}$ such that $s_r \in K[t, a_1, \ldots, a_r]$ is squarefree and $\deg_t s_r = 2M$. Hence $\Delta_t(s_r) \neq 0$ in $K[a_1, \ldots, a_r]$. So there exist $\bar{a}_1, \ldots, \bar{a}_r \in K$ such that $(x_r)_i(t, \bar{a}_1, \ldots, \bar{a}_r) \neq 0$ for all $i \in \{1, \ldots, 7\}$, $\deg s_r(t, \bar{a}_1, \ldots, \bar{a}_r) = 2M$ and $\Delta_t(s_r(t, \bar{a}_1, \ldots, \bar{a}_r)) \neq 0$. So we have that the vector $((x_r)_1(t, \bar{a}_1, \ldots, \bar{a}_r), \ldots, (x_r)_7(t, \bar{a}_1, \ldots, \bar{a}_r))$ is an isotropic vector of q over $K[t]$, such that $\deg s_r = 2M$ and $s_r(t, \bar{a}_1, \ldots, \bar{a}_r)$ is squarefree. □

3.5 Isotropy over rational function fields over algebraic subfields of p-adic fields

Let K be a p-adic field with uniformizer π and $\gamma \in K^*$. Let $g \in K[t]$ with $g(0) \neq 0$. From Corollary 3.3.8 we know that if all the vertices of the Newton polygon of g

have even degree, then the quadratic form

$$q = \langle 1, \pi \rangle \langle 1, -\gamma, -t \rangle \perp \langle -g \rangle$$

is isotropic over $K(t)$.

Our goal is to prove the analogous result for K a subfield of a p-adic field that is algebraic over $\mathbb{Q}$. The reason why we restrict ourselves to subfields of a p-adic field, is that we want to find $\pi, \gamma \in K^*$ such that $\langle 1, \pi \rangle \langle 1, -\gamma \rangle$ is anisotropic over K. In Lemma 3.5.5 we prove that we can find such π and γ, with also some extra conditions. Then we want to find an isotropic vector of q over $K[t]$ by approximating an isotropic vector over $K_\mathfrak{p}[t]$, where $K_\mathfrak{p}$ is a completion of K at a valuation $v_\mathfrak{p}$ such that $v_\mathfrak{p}(\pi)$ odd. To be able to approximate simultaneously isotropic vectors over different completions, we use the isotropic vector over $K_\mathfrak{p}[t]$ that we found in Theorem 3.4.5. These local isotropic vectors are then used to construct a global isotropic vector in Theorem 3.5.6.

Definition 3.5.1. Let K be a field, $\bar{K}$ a fixed algebraic closure of K. A polynomial $f \in K[t]$ is called *separable* if all its roots in $\bar{K}$ are distinct.

Lemma 3.5.2 (Krasner's Lemma). *Let K be field, complete with respect to a valuation v. Let $\alpha \in \bar{K}$, separable over K, and let $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_n$ be the conjugates of α over K. Denote the unique extension of v to $\bar{K}$ also with v. Suppose that for $\beta \in \bar{K}$ the following holds:*

$$v(\beta - \alpha) > v(\alpha - \alpha_i) \qquad \text{for all } i \geq 2.$$

Then $K(\alpha) \subseteq K(\beta)$.

Proof. See [NSW00, Chapter VIII, Lemma 8.1.6]. □

Proposition 3.5.3. *Let K be field, complete with respect to a valuation v. Let $f = a_0 + a_1 t + \cdots + a_d t^d \in K[t]$ be a separable polynomial. Then there exists an integer M_f such that for all $g = b_0 + b_1 t + \cdots + b_d t^d \in K[t]$ with*

$$v(f - g) := \min_j (v(a_j - b_j)) > M_f,$$

holds that g is also separable and that there exists a bijection $\alpha_i \mapsto \beta_{j(i)}$ between the roots α_i of f in $\bar{K}$ and the roots β_j of g in $\bar{K}$ such that $K(\alpha_i) = K(\beta_{j(i)})$.

Proof. This follows from the proof for [NSW00, Chapter XII, Lemma 12.1.1]. Let $\alpha \in \bar{K}$ be a root of f. If g is close to f, then $v(g(\alpha)) = v((f-g)(\alpha)) \geq \min\{v(a_d - b_d) + dv(\alpha), \ldots, v(a_0 - b_0)\}$ is large. Writing $g = b_d \prod_{j=1}^{d}(t - \beta_j)$, then $v(g(\alpha)) = v(b_d) + \sum_j v(\alpha - \beta_j)$, and we have that $v(\alpha - \beta)$ is large for some root β of g. In particular, for g such that $v(f-g)$ is sufficiently large, we can choose a root β of g such that $v(\beta - \alpha) > v(\alpha - \alpha_i)$ for all other roots $\alpha_i \neq \alpha$ of f. From Lemma 3.5.2 follows that $K(\alpha) \subseteq K(\beta)$. We can repeat the reasoning above to find for each root α_i of f, a root $\beta_{j(i)}$ of g, such that $v(\beta_{j(i)} - \alpha_i) > v(\alpha_l - \alpha_i)$ for all $l \neq i$. For all i, k with $i \neq k$ we have that

$$v(\alpha_i - \alpha_k) \geq \min\{v(\alpha_i - \beta_{j(i)}), v(\beta_{j(i)} - \beta_{j(k)}), v(\beta_{j(k)} - \alpha_k)\}.$$

Since $v(\alpha_i - \beta_{j(i)}) > v(\alpha_i - \alpha_k)$ and $v(\beta_{j(k)} - \alpha_k) > v(\alpha_i - \alpha_k)$, we have that $v(\alpha_i - \alpha_k) \geq v(\beta_{j(i)} - \beta_{j(k)})$. Since $\alpha_i - \alpha_k \neq 0$, it follows that $\beta_{j(i)} \neq \beta_{j(k)}$, so g is separable. So for g such that $v(f-g)$ is sufficiently large, we have a bijection $\alpha_i \mapsto \beta_{j(i)}$ between the roots α_i of f and the roots β_j of g, such that

$$v(\beta_{j(i)} - \alpha_i) > v(\alpha_i - \alpha_k) \geq v(\beta_{j(i)} - \beta_{j(k)})$$

for all $i \neq k$. Applying again Lemma 3.5.2, we find that $K(\beta_{j(i)}) \subseteq K(\alpha_i)$. □

Definition 3.5.4. Let K be an algebraic extension of $\mathbb{Q}$. An element $\alpha \in K^*$ is said to be *totally negative* if $\varphi(\alpha) < 0$ for every embedding $\varphi : K \hookrightarrow \mathbb{R}$. (Remark that if K is not a real field, this condition is vacuously satisfied.)

From now on, let K be a subfield of a p-adic field L and suppose $K/\mathbb{Q}$ is algebraic. The restriction of the p-adic valuation on L is a valuation $v_\mathfrak{p}$ on K that extends the p-adic valuation v_p on $\mathbb{Q}$. Let $K_\mathfrak{p}$ be the completion of K at $v_\mathfrak{p}$. The embedding of K in L extends to an embedding of $K_\mathfrak{p}$ in L. We also have that $K_\mathfrak{p} = \cup F_\mathfrak{p}$ is the union of the completions $F_\mathfrak{p}$ at $v_\mathfrak{p}$ of all finite subextensions $F/\mathbb{Q}$ of K.

Lemma 3.5.5. *Let K be a subfield of a p-adic field, $K/\mathbb{Q}$ algebraic. There exist $\pi, \gamma \in K^*$ such that the following hold*

1. *$\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over K,*
2. *π is totally negative,*

3. *let $E \subset K$ be a subfield such that $E/\mathbb{Q}$ is finite and $\pi, \gamma \in E$. Let $\mathfrak{B}$ be a finite prime of E such that $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over $E_{\mathfrak{B}}$. Then $v_{\mathfrak{B}}(\pi)$ is odd.*

Proof. Let $\tilde{\gamma} \in O_{K_{\mathfrak{p}}}^{\times}$ such that $K_{\mathfrak{p}}(\sqrt{\tilde{\gamma}})$ is unramified. There exist a finite subextension $F/\mathbb{Q}$ of K, such that $\tilde{\gamma} \in F_{\mathfrak{p}}$. Choose $\gamma \in F^*$ such that $v_{\mathfrak{p}}(\gamma - \tilde{\gamma})$ is very large, from Lemma 3.5.3 follows that $K_{\mathfrak{p}}(\sqrt{\gamma}) \cong K_{\mathfrak{p}}(\sqrt{\tilde{\gamma}})$. Let $\tilde{\pi} \in K^*$ be a uniformizer for $v_{\mathfrak{p}}$, and $M = \mathbb{Q}(\gamma, \tilde{\pi})$. With weak approximation [EP05, Theorem 1.1.3] we find $\pi \in M^*$ such that $v_{\mathfrak{p}}(\pi) = 1$, π is totally negative, and $v_{\mathfrak{q}}(\pi)$ is odd for all primes $\mathfrak{q}$ of M such that $v_{\mathfrak{q}}(2) \neq 0$ or $v_{\mathfrak{q}}(\gamma) \neq 0$. Since π is also a uniformizer for $v_{\mathfrak{p}}$ and $K_{\mathfrak{p}}(\sqrt{\gamma})$ is unramified, $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over $K_{\mathfrak{p}}$, so $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over K.

Now consider $\mathbb{Q}(\pi, \gamma)$. From the way we chose π, it follows that for every finite prime $\mathfrak{q}$ of $\mathbb{Q}(\pi, \gamma)$ such that $v_{\mathfrak{q}}(2) \neq 0$ or $v_{\mathfrak{q}}(\gamma) \neq 0$, we have that $v_{\mathfrak{q}}(\pi)$ is odd. Let $E \subset K$ be a subfield that is finite over $\mathbb{Q}$, and such that $\mathbb{Q}(\pi, \gamma) \subseteq E$. Let $\mathfrak{Q}$ be a finite prime of E such that $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over $E_{\mathfrak{Q}}$. Let $\mathfrak{q}$ be the prime of $\mathbb{Q}(\pi, \gamma)$ such that $\mathfrak{Q} \mid \mathfrak{q}$. Suppose that $v_{\mathfrak{q}}(\pi)$ is even, then by our choice of π, it follows that $v_{\mathfrak{q}}(\gamma) = 0$ and $v_{\mathfrak{q}}(2) = 0$. Therefore the form $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is isotropic at $\mathfrak{q}$, a contradiction. So $v_{\mathfrak{q}}(\pi)$ is odd. We now claim that then also follows that $v_{\mathfrak{Q}}(\pi)$ is odd. Otherwise it would mean that $\mathfrak{q}$ ramifies in E with even ramification degree, so $[E_{\mathfrak{Q}} : \mathbb{Q}(\pi, \gamma)_{\mathfrak{q}}]$ is even, hence from [Rei03, Chapter 7, Corollary 31.10] follows that $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is isotropic over $E_{\mathfrak{Q}}$, a contradiction. □

Let F be a number field. For a finite prime $\mathfrak{p}$ of F, the Newton polygon of g at $\mathfrak{p}$, is the Newton polygon of g considered as a polynomial over $F_{\mathfrak{p}}$.

Theorem 3.5.6. *Let K be a a subfield of a p-adic field, $K/\mathbb{Q}$ algebraic. Let $\pi, \gamma \in K^*$ as in Lemma 3.5.5. Let $g \in K[t]$ with $g(0) \neq 0$. Suppose that for all the valuations v on K such that $v(\pi)$ is odd, the vertices of the Newton polygon of g at v have even degree, then the quadratic form*

$$q = \langle 1, \pi\rangle\langle 1, -\gamma, -t\rangle \perp \langle -g\rangle$$

is isotropic over $K(t)$.

Proof. We can assume that g is a squarefree polynomial (dividing out squared factors does neither change the isotropy of q, nor the condition that the vertices

of the Newton polygon have even degree). Let F be the number field generated by π, γ and the coefficients of g.

Suppose that $g \in K$. Then $\langle 1, \pi\rangle\langle 1, -\gamma, -g\rangle$ is isotropic over $F_{\mathfrak{P}}$, for every finite prime $\mathfrak{P}$ of F. Since π is totally negative, $\langle 1, \pi\rangle\langle 1, -\gamma, -g\rangle$ is also isotropic over every $F_{\mathfrak{P}} \cong \mathbb{R}$. From the Hasse-Minkowski principle 3.1.7 follows that $\langle 1, \pi\rangle\langle 1, -\gamma, -g\rangle$ is isotropic over F. Hence q is isotropic over $F(t)$.

Now suppose that $\deg g \geq 1$. We only need to consider the set of primes of F

$$\mathcal{P} = \{\mathfrak{P} \mid \langle 1, \pi\rangle\langle 1, -\gamma\rangle \text{ is anisotropic over } F_{\mathfrak{P}}\}.$$

Since $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is isotropic over $F_{\mathfrak{P}}$ for all primes $\mathfrak{P}$ such that $v_{\mathfrak{P}}(\pi) = 0$, $v_{\mathfrak{P}}(\gamma) = 0$ and $v_{\mathfrak{P}}(2) = 0$, and for all real primes, $\mathcal{P}$ is a finite set of finite primes. From Lemma 3.5.5 follows that for every $\mathfrak{P} \in \mathcal{P}$, we have that $v_{\mathfrak{P}}(\pi)$ is odd, and that the vertices of the Newton polygon of g have even degree, so from Corollary 3.3.8 follows that the quadratic form $q = \langle 1, \pi\rangle\langle 1, -\gamma, -t\rangle \perp \langle -g\rangle$ is isotropic over $F_{\mathfrak{P}}(t)$. Let $(x_1^{\mathfrak{P}}, \ldots, x_7^{\mathfrak{P}})$ be an isotropic vector of q with all $x_i \in F_{\mathfrak{P}}[t]$. Now let $m = \max_{\mathfrak{P}}(\max_{i=1,\ldots,4} \deg x_i^{\mathfrak{P}})$. Take $M \in \mathbb{N}$, $2M \geq 2m + 20$. Then from Theorem 3.4.5 follows that there exists an isotropic vector $(y_1^{\mathfrak{P}}, \ldots, y_7^{\mathfrak{P}})$ of q with $y_i^{\mathfrak{P}} \in F_{\mathfrak{P}}[t]$ such that $s^{\mathfrak{P}} := (y_1^{\mathfrak{P}})^2 + \pi(y_2^{\mathfrak{P}})^2 - \gamma(y_3^{\mathfrak{P}})^2 - \pi\gamma(y_4^{\mathfrak{P}})^2 \neq 0$ is squarefree and $\deg s^{\mathfrak{P}} = 2M$. Now let $x_5, x_6, x_7 \in F[t]$ such that $v_{\mathfrak{P}}(x_i - x_i^{\mathfrak{P}})$ is large for every $\mathfrak{P} \in \mathcal{P}$.

Let $s := tx_5^2 + \pi t x_6^2 + g x_7^2$, then by construction of s, the quadratic form $\langle t, \pi t, g, -s\rangle$ is isotropic over $F(t)$. This is a subform of the quadratic form $\langle 1, \pi\rangle\langle t, g\rangle\langle 1, -ts\rangle$, therefore we have that

$$\langle 1, \pi\rangle\langle 1, tg\rangle\langle 1, -ts\rangle$$

is isotropic over $F(t)$.

Now consider the quadratic form

$$\varphi = \langle 1, \pi\rangle\langle 1, -\gamma\rangle\langle 1, -s\rangle.$$

By a similar reasoning as in Proposition 3.3.2, it suffices to prove that $\delta_p(\varphi)$ is hyperbolic for monic irreducible polynomials p in $F[t]$ to prove global isotropy. Namely, if all the second residue maps of φ are zero, then φ is Witt equivalent to an anisotropic form ψ over F. Now, suppose for the sake of contradiction that φ

is anisotropic over $F(t)$, then $\psi \cong \varphi$ over $F(t)$. From this follows that $\dim \psi = 8$, so ψ is isotropic over all $F_{\mathfrak{p}}$, with $\mathfrak{p}$ a finite prime. Since ψ is anisotropic over F, it follows from the Hasse-Minkowski principle 3.1.7 that there exists a real prime σ such that ψ is anisotropic over $F_\sigma \cong \mathbb{R}$, hence ψ is anisotropic over $F_\sigma(t)$. But since π is totally negative, φ is isotropic over $F_\sigma(t)$, so ψ would be isometric to a form of lower dimension, a contradiction.

Since the second residue map of φ is trivially zero, except at the irreducible factors of s, we have to verify that $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is isotropic over $F[t]/(a(t))$ for each monic irreducible factor $a(t)$ of $s(t)$. Let $L = F[t]/(a(t))$, then by the Hasse-Minkowski principle 3.1.7, $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is isotropic over L if and only if $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is isotropic over L_ρ, for each prime ρ. First, let ρ be a prime such that $\rho \mid \mathfrak{P}$, with $\mathfrak{P} \in \mathcal{P}$. We have that $L_\rho \cong F_{\mathfrak{P}}[t]/(\alpha(t))$ for a monic irreducible factor $\alpha(t) \in F_{\mathfrak{P}}[t]$ of $s(t)$. Since s is close to $s^{\mathfrak{P}}$ and $s^{\mathfrak{P}}$ is squarefree, it follows from Proposition 3.5.3 that there exists a factor $\alpha^{\mathfrak{P}}$ of $s^{\mathfrak{P}}$ such that $L_\rho \cong F_{\mathfrak{P}}[t]/(\alpha) = F_{\mathfrak{P}}[t]/(\alpha^{\mathfrak{P}})$. Since $s^{\mathfrak{P}} \equiv (y_1^{\mathfrak{P}})^2 + \pi(y_2^{\mathfrak{P}})^2 - \gamma(y_3^{\mathfrak{P}})^2 - \pi\gamma(y_4^{\mathfrak{P}})^2 \equiv 0 \mod a^{\mathfrak{P}}$ and $s^{\mathfrak{P}}$ is squarefree, it follows that $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is isotropic over $F_{\mathfrak{P}}[t]/(\alpha^{\mathfrak{P}}) \cong L_\rho$. Now let ρ be a prime that does not lie above a prime in $\mathcal{P}$, $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is isotropic over L_ρ by definition of $\mathcal{P}$.

Analogous to the proof of Corollary 3.3.8, the isotropy of the quadratic forms $\langle 1, \pi\rangle\langle 1, -\gamma\rangle\langle 1, -s\rangle$ and $\langle 1, \pi\rangle\langle 1, tg\rangle\langle 1, -ts\rangle$, implies the isotropy of

$$\langle 1, \pi\rangle\langle 1, -\gamma, -t\rangle \perp \langle -g\rangle$$

over $F(t)$, hence also over $K(t)$. □

Chapter 4

Diophantine definition of the valuation ring

In this chapter, we prove one of our main results, namely undecidability for diophantine equations over $K(t)$, for K a p-adic field or for K an algebraic subfield of a p-adic field (see Corollary 4.1.7). For a rational function field $K(t)$, proving that Hilbert's Tenth Problem has a negative answer, can be reduced to giving a diophantine definition of the valuation ring of v_∞. We give such a diophantine definition in this chapter, using the results on the isotropy of our class of quadratic forms from the previous chapters.

An important subset of a rational function field $K(t)$ is the set of constants. When K is a p-adic field, we can use elliptic curves to prove that this set is diophantine over $K(t)$.

Proposition 4.1.1. *Let K be a p-adic field, then K is diophantine in $K(t)$.*

Proof. Let E be the elliptic curve over K given by the equation $y^2 = x^3 - x$. Let $b \in K$ with $v(b) > 0$. We claim that there is an $a \in K$ such that (a, b) lies on $E(K)$. Let $f(x) = x^3 - x - b^2 \in O[x]$. Since $v(f(0)) = 2v(b) > 0 = 2v(f'(0))$, it follows from Theorem 1.1.2 that there exists an $a \in O$ such that $f(a) = 0$. So

$$K = \{b_1/b_2 \mid (\exists a_1, a_2 \in K)((a_1, b_1) \in E(K) \ \wedge \ (a_2, b_2) \in E(K) \ \wedge \ b_2 \neq 0)\}.$$

By Hurwitz' Theorem [Har77, Chapter IV, Corollary 2.4], the curve $y^2 = x^3 - x$ admits no rational parametrization, so $E(K(t)) = E(K)$. This means

$$K = \{b_1/b_2 \mid (\exists a_1, a_2 \in K(t))((a_1, b_1) \in E(K(t)) \ \wedge \ (a_2, b_2) \in E(K(t)) \ \wedge \ b_2 \neq 0)\}$$

hence K is diophantine in $K(t)$. □

Remark 4.1.2. We now fix notations for a set of prime numbers V and a certain set $U \subseteq K$, in the cases that K is an algebraic subfield of a p-adic field and that K is a p-adic field. We also fix notations for elements $\pi, \gamma \in K^*$ such that the quadratic form $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over K.

1. Let K be an algebraic subfield of a p-adic field. By Lemma 3.5.5, there exists $\pi, \gamma \in K^*$ such that $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over K. Furthermore, π is totally negative and for all subfields $E \subset K$ such that $E/\mathbb{Q}$ is finite, if $\mathfrak{p}$ is a finite prime of E such that $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over $E_\mathfrak{p}$, it follows that $v_\mathfrak{p}(\pi)$ is odd. Let $V = \{p_i \mid i = 1, \dots, r\}$, with p_i the prime numbers such that $v(\pi) \neq 0$ for some valuation v on K that extends v_{p_i}. From [KR95, Proposition 3] follows that there exists a set $U \subseteq K$ such that U is diophantine in $K(t)$ and such that $U \cap \mathbb{Q}$ is dense in $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_r}$. This was also proved by Eisenträger in greater generality in [Eis07, Theorem 5.5].

2. Let K be a p-adic field. Let π be a fixed uniformizer. By [Lam05, Chapter VI, Corollary 2.15], there exists a $\gamma \in K^*$, such that $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ is anisotropic over K. Let $V := \{p\}$, where p is a prime number such that K is a finite extension of $\mathbb{Q}_p$. We let $U := K$. The set U is diophantine in $K(t)$ by Proposition 4.1.1.

Throughout this section, we work with the following system of two quadratic forms over $K(t)$:

$$\langle 1, \pi\rangle\langle 1, -\gamma, -t\rangle \perp \langle -f\rangle \tag{4.1}$$
$$\langle 1, \pi\rangle\langle 1, -\gamma, -t\rangle \perp \langle -\gamma f\rangle. \tag{4.2}$$

with $f \in K(t)$. First, we prove a theorem which is analogous to [KR95, Proposition

7]. The quadratic forms above are analogous[1] to the quadratic forms appearing in the cited Proposition.

Theorem 4.1.3. *Let $f \in K(t)$. If $v_\infty(f)$ is odd, then one of the quadratic forms* (4.1) *or* (4.2) *is anisotropic over $K(t)$.*

Proof. Let $f = \frac{f_1}{f_2}$ with $f_1, f_2 \in K[t]$, $f_2 \neq 0$. By assumption, $\deg f_2 - \deg f_1$ is odd. Denote the leading coefficient of f_i with $c_i \in K^*$, let $c := c_1/c_2$. The first and second residue class forms of (4.1) of v_∞ are $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ and $\varphi_1 := -\langle 1, \pi\rangle \perp \langle -c\rangle$. The residue forms of (4.2) at v_∞ are $\langle 1, \pi\rangle\langle 1, -\gamma\rangle$ and $\varphi_2 := -\langle 1, \pi\rangle \perp \langle -\gamma c\rangle$. By assumption $\langle 1, \pi\rangle\langle 1, -\gamma\rangle \neq 0$ in $W(K)$. Let $\psi_1 = \langle 1, \pi\rangle\langle -1, -c\rangle$ and $\psi_2 = \langle 1, \pi\rangle\langle -1, -\gamma c\rangle$. Since

$$\begin{aligned}\psi_2 - \psi_1 &= \langle 1, \pi\rangle\langle -1, -\gamma c, 1, c\rangle \\ &= \langle c\rangle\langle 1, \pi\rangle\langle 1, -\gamma\rangle \neq 0 \quad \text{in } W(K),\end{aligned}$$

it follows that $\psi_1 \neq 0$ or $\psi_2 \neq 0$. Suppose that $\psi_1 \neq 0$ (the argument for $\psi_2 \neq 0$ is completely analogous). Since ψ_1 is a Pfister form, it follows from Theorem 3.1.4 that ψ_1 is anisotropic. Therefore φ_1 is anisotropic, so both residue forms of (4.1) are anisotropic, hence (4.1) is anisotropic. □

We prove a consequence of Theorem 3.3.8 (for p-adic fields) and Theorem 3.5.6 (for algebraic subfields of p-adic fields). Roughly speaking, we start from a given rational function $h \in K(t)$ and we construct a polynomial such that the vertices of its Newton polygon at the valuations v with $v \in V$, have even degree.

Theorem 4.1.4. *Let $h \in K(t)$ be such that $v_\infty(h) \geq -2$ and $v_t(h) = 0$. Let U be as before in Remark 4.1.2. Then there exists $c \in U$ such that, if we let*

$$f := h + ct^2, \tag{4.3}$$

both quadratic forms (4.1) *and* (4.2) *are isotropic over $K(t)$.*

Proof. Since $v_\infty(h) \geq -2$ and $v_t(h) = 0$, we can write $h(t) = \frac{h_N(t)}{h_D(t)}$ with h_N and h_D polynomials such that $h_N(0)h_D(0) \neq 0$ and $\deg h_N \leq \deg h_D + 2$. Multiplying

[1] The letter b from Kim and Roush corresponds to our π; a corresponds to our γ; f corresponds to $t \cdot g$, the forms are multiplied with a factor $\langle t\rangle$ and we work with 7-dimensional instead of 8-dimensional forms.

f with h_D^2 does not change the isotropy of (4.1) and (4.2). We want to apply Corollary 3.3.8 (in the case that K is a p-adic field) or Theorem 3.5.6 (in the case that K is an algebraic subfield of a p-adic field) with $g = fh_D^2$, so

$$g = h_N h_D + ct^2 h_D^2.$$

It is clear that $g(0) \neq 0$ and $\deg g = 2 + 2 \deg h_D$.

Let V be as before in Remark 4.1.2. We will choose $c \in K$ such that $v(c)$ is very low for all valuations v that extend v_p for all $p \in V$ (depending on the coefficients of h_N and h_D). We choose $v_p(c)$ so low that the first edge of the Newton polygon of g at v has vertices of degree 0 and degree 2. Choosing $v(c)$ low enough, the remaining vertices of the Newton polygon of g at v are the vertices of the Newton polygon of $ct^2h_D^2$, and those also have even degree. To do this, we choose $c \in \mathbb{Q} \cap U$ such that $v_p(c)$ is very low for every $p \in V$, since $U \cap \mathbb{Q}$ is dense in $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_r}$, with $p_i \in V$. So g satisfies the conditions of Corollary 3.3.8 or Theorem 3.5.6, and because multiplying g with $\gamma \in K^*$ does not change the degree of the vertices of g, the isotropy of (4.1) and (4.2) follows. □

We prove the next theorem similar to [Dem10, Proposition 4.7], in which we relate the valuation v_∞ to the isotropy of our system of quadratic forms.

Theorem 4.1.5. *Let $x \in K(t)$. Then $v_\infty(x) \geq 0$ if and only if there exists a $c \in U$ such that the quadratic forms (4.1) and (4.2) are isotropic with*

$$f := \frac{t^4 + t^3x^5 + x^5}{t^4 + x^5} + ct^2.$$

Proof. Define $h_N := t^4 + t^3x^5 + x^5$, $h_D := t^4 + x^5$ and $h := h_N/h_D$.

Assume first that $v_\infty(x) \geq 0$. Then $v_\infty(h_N) = -4$ and $v_\infty(h_D) = -4$ such that $v_\infty(h) = 0$. If $v_t(x) \geq 1$, then $v_t(h_N) = 4$ and $v_t(h_D) = 4$ such that $v_t(h) = 0$. If $v_t(x) \leq 0$, then $v_t(h_N) = 5v_t(x)$ and $v_t(h_D) = 5v_t(x)$ such that $v_t(h) = 0$. In short, if $v_\infty(x) \geq 0$, then $v_\infty(h) = 0$ and $v_t(h) = 0$. Theorem 4.1.4 gives us that there exists a $c \in U$ such that (4.1) and (4.2) are isotropic.

Conversely, assume that $v_\infty(x) \leq -1$. Then $v_\infty(h_N) = -3 + 5v_\infty(x)$ and $v_\infty(h_D) = 5v_\infty(x)$ such that $v_\infty(h) = -3$. It follows that $v_\infty(f) = -3$. By Theorem 4.1.3, for every $c \in U$, one of the quadratic forms (4.1) and (4.2) is anisotropic. □

Corollary 4.1.6. *In $K(t)$, the relation $v_\infty(x) \geq 0$ is diophantine.*

Proof. Since quadratic forms being isotropic is a diophantine condition and U is diophantine in $K(t)$, the result follows immediately from Theorem 4.1.5. □

Corollary 4.1.7. *Let K be a p-adic field or an algebraic subfield of a p-adic field. Then diophantine equations over $K(t)$ are undecidable.*

Proof. This follows immediately from Theorem 2.3.1 and Corollary 4.1.6. □

Part II

Diophantine sets over polynomial rings

Chapter 5

Recursively enumerable sets

In this chapter, we give the necessary definitions concerning recursive and recursively enumerable sets (r.e.) in the natural numbers, and we show how the negative answer to Hilbert's Tenth Problem for the integers follows from the DPRM-theorem (namely, that r.e. sets are diophantine). Since we want to examine the equivalence between r.e. sets and diophantine sets in other rings, we also show how one can define the notion of an r.e. set in a recursive ring.

In the literature, one also encounters the terms listable or computably enumerable set for recursively enumerable set, and computable set for recursive set. Other terms that are used for recursive ring are computable ring, recursively presentable ring, constructive ring and explicit ring.

5.1 Recursively enumerable sets and Hilbert's Tenth Problem

Definition 5.1.1. A set $A \subseteq \mathbb{N}^k$ is *recursively enumerable* (or short r.e.) if there exists an algorithm that prints the elements of A. Each element of A is hereby printed at least once, and no elements that are not in A are printed. The algorithm can run infinitely long and can use an unbounded amount of memory.

Definition 5.1.2. Let k be a natural number. A set $A \subseteq \mathbb{N}^k$ is *recursive* if there exists an algorithm that, on input $a \in \mathbb{N}^k$, decides whether $a \in A$.

So recursively enumerable sets and recursive sets are defined for subsets of the natural numbers, but it makes little difference if we also use the notion for subsets of the integers.

It is clear that diophantine sets are recursively enumerable. Indeed, let $A \subset \mathbb{Z}^k$ be a diophantine set, given by the equation $f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0$. The following algorithm prints the elements of A: loop over all possible elements $(a_1, \ldots, a_k, x_1, \ldots, x_n) \in \mathbb{Z}^{k+n}$, test whether $f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0$, and print $(a_1, \ldots, a_k)$ if the answer is yes.

Every recursive set A is also recursively enumerable, since we can consider the algorithm that runs over the natural numbers $n \in \mathbb{N}$, decides whether $n \in A$, and when the outcome of that decision algorithm is positive, prints n. However, the converse is not true.

Theorem 5.1.3. *There exists a set $S \subset \mathbb{N}$ that is r.e. but the complement $\mathbb{N} \setminus S$ is not r.e.*

This fact, together with the DPRM-theorem that says that every recursively enumerable set $A \subseteq \mathbb{Z}^k$ is diophantine, proves the negative answer to Hilbert's Tenth Problem.

Theorem 5.1.4 (DPRM-theorem). *A subset $A \subseteq \mathbb{Z}^k$ is recursively enumerable if and only if A is diophantine over $\mathbb{Z}$.*

Corollary 5.1.5. *Diophantine equations over $\mathbb{Z}$ are undecidable.*

Proof. Let S be an r.e. set in $\mathbb{Z}$, with $\mathbb{Z} \setminus S$ not r.e. . From DPRM follows that S is diophantine, so there exists $n \in \mathbb{N}$ and $f \in \mathbb{Z}[a, x_1, \ldots, x_n]$ such that $S = \{a \in \mathbb{Z} \mid (\exists x_1, \ldots, x_n \in \mathbb{Z})\, f(a, x_1, \ldots, x_n) = 0\}$. Suppose diophantine equations over $\mathbb{Z}$ were decidable, then we could decide whether a is in S. So S would be recursive, a contradiction. □

5.2 Recursive rings

To prove that r.e. sets are diophantine for other rings than $\mathbb{Z}$, we have to transfer the notion of recursively enumerable sets to a countable ring R. This will only work if it is possible to effectively compute in R, i.e. if R is a recursive ring. The idea of a recursive ring is that each element $a \in R$ has a code $\sigma(a) \in \mathbb{N}$. Given the codes $\sigma(a)$ and $\sigma(b)$ of $a, b \in R$, a computer has to be able to compute the codes $\sigma(a+b)$ and $\sigma(ab)$.

Definition 5.2.1. We call R a *recursive ring* if R is a ring with a bijection $\sigma : R \xrightarrow{\sim} \mathbb{N}$ such that the sets

$$R_+^\sigma = \{(\sigma(a), \sigma(b), \sigma(a+b)) \mid a, b \in R\} \subseteq \mathbb{N}^3$$
$$R_\times^\sigma = \{(\sigma(a), \sigma(b), \sigma(ab)) \mid a, b \in R\} \subseteq \mathbb{N}^3$$

are recursive subsets of $\mathbb{N}^3$. Then σ is called a *recursive presentation* of R.

Examples 5.2.2. We give some examples of recursive rings.

1. The field $\mathbb{Q}$ of rationals is recursive, as well as any finite extension of $\mathbb{Q}$.
2. The real closure and algebraic closure of $\mathbb{Q}$ are recursive.
3. Let $\mathcal{S} \subseteq \mathbb{N}$ be a subset of the prime numbers and let $L = \mathbb{Q}(\{\sqrt{p} \mid p \in \mathcal{S}\})$. Then L is a recursive field if and only if $\mathcal{S}$ is recursively enumerable.

   Proof. Suppose there exists a recursive presentation $\sigma : L \xrightarrow{\sim} \mathbb{N}$. The set of primes is recursive, so we can list the codes of the prime numbers $\sigma(p_0), \sigma(p_1), \ldots$. Now we loop over all pairs (e, p_n) with $e \in L$, and we check whether $(\sigma(e), \sigma(e), \sigma(p_n)) \in L_\times^\sigma$. If we find such a pair, we print p_n. Since we print those p_n such that there exists an $e \in L$ with $e^2 = p_n$, $\mathcal{S}$ is recursively enumerable.

   Let $\mathcal{S}$ be recursively enumerable and $L = \mathbb{Q}(\{\sqrt{p} \mid p \in \mathcal{S}\})$. If $\mathcal{S}$ is finite, then $L/\mathbb{Q}$ is a finite extension and hence recursive. Now suppose that $\mathcal{S}$ is an infinite set. We will give an algorithm that constructs L as a chain of finite extensions $L_0 := \mathbb{Q} \subset L_1 \subset L_2 \subset \ldots$ such that $L = \cup_i L_i$. This works since we construct in each step a finite extension $L_i/\mathbb{Q}$. Then later, if we wish to compute the sum or product of two elements $a, b \in L$ for

this recursive presentation, we let the algorithm run until it defines L_i such that $a, b \in L_i$, and then we computed the desired sum or product in L_i. The algorithm that builds L now goes as follows: let the algorithm run that prints the elements of $\mathcal{S}$. Whenever a new element p is printed, let $L_i = L_{i-1}(\sqrt{p})$. □

4. If R is a recursive ring, then the polynomial ring $R[t]$ is recursive ([FS56, Theorem 3.1]). Moreover, let ι be the natural embedding $R \hookrightarrow R[t]$. Given a recursive presentation $\sigma : R \tilde{\to} \mathbb{N}$, there exists a recursive presentation $\tau : R[t] \tilde{\to} \mathbb{N}$ such that $\tau \circ \iota \circ \sigma^{-1}$ is recursive and such that $\iota(R) \subset R[t]$ is a recursive set w.r.t. τ. Intuitively, this means that we can freely mix computations in R and $R[t]$.

We follow [SHT99, Definition 2.2.4] for the definition of a recursively stable ring.

Definition 5.2.3. A recursive ring R is called *recursively stable* if for any two recursive presentations $\sigma : R \tilde{\to} \mathbb{N}$ and $\tau : R \tilde{\to} \mathbb{N}$, the set $\{(\sigma(r), \tau(r)) \in \mathbb{N}^2 \mid r \in R\}$ is recursive.

Equivalently, "recursively stable" means that, given any two recursive presentations σ and τ, there exists a recursive permutation $\pi : \mathbb{N} \tilde{\to} \mathbb{N}$ such that $\tau = \pi \circ \sigma$.

Examples 5.2.4. We give some examples of recursively stable rings.

1. The field $\mathbb{Q}$ of rationals is recursively stable, as well as any finite extension of $\mathbb{Q}$.

2. Let $\sigma : R \tilde{\to} \mathbb{N}$ be a recursive presentation of a ring R and $\varphi \in \mathrm{Aut}(R)$. Then $\sigma \circ \varphi$ is again a recursive presentation (with the same sets R^σ_+ and $R^\sigma_\times$). If R is recursively stable, then $\sigma \circ \varphi \circ \sigma^{-1} : \mathbb{N} \tilde{\to} \mathbb{N}$ must be recursive. Since there exist only countably many recursive functions, any ring with uncountably many automorphisms (such as $\bar{\mathbb{Q}}$) cannot be recursively stable.

3. If R is recursively stable, then the polynomial ring $R[t]$ is also recursively stable.

Using a recursive presentation, we can now define recursively enumerable subsets of a ring R.

Definition 5.2.5. Let R be a recursive ring with recursive presentation $\sigma : R \tilde{\to} \mathbb{N}$. A set $A \subseteq R^k$ is defined to be *recursively enumerable* if the set

$$\{(\sigma(a_1), \ldots, \sigma(a_k)) \in \mathbb{N}^k \mid (a_1, \ldots, a_k) \in A\}$$

is an r.e. subset of $\mathbb{N}^k$.

A priori, this definition may depend on the chosen recursive presentation. However, if R is recursively stable, it does not depend on the recursive presentation. For rings which are not recursively stable, we can still consider the sets that are r.e. *for every recursive presentation*. This is what we will do in the next Chapters, where we will consider r.e. sets in the polynomial ring $L[t]$, with $L/\mathbb{Q}$ an algebraic extension. Since $L[t]$ is not necessarily recursively stable, whether a set is r.e. might depend on the recursive presentation. However, diophantine subsets are r.e. for every recursive presentation. Therefore, if we want to prove that r.e. sets are diophantine for $L[t]$, we have to restrict ourselves to sets that are r.e. for every recursive presentation.

Chapter 6

Automorphism-recursive fields

In this chapter, we consider recursive algebraic extensions L of $\mathbb{Q}$, and recursively enumerable sets in $L[t]$ that are r.e. for every recursive presentation. In Section 6.3, we characterize these sets algebraically, using automorphisms of L. To do this, we need to know more about these automorphisms in an algorithmic sense. Therefore, we introduce in Section 6.2 the concept of an *automorphism-recursive field*. In an automorphism-recursive field, we can compute, given an element $\alpha \in L$, the set $\{\varphi(\alpha) \mid \varphi \in \mathrm{Aut}(L)\}$. However, the notion of automorphism-recursive is stronger than this, as we will show in Section 6.4.

6.1 Refining minimal polynomials

Let F be a field and L a separable algebraic extension of F. In this short section, we first prove a proposition concerning the extension of field embeddings. Let $\bar{F}$ be a fixed algebraic closure of F. The $\mathrm{Aut}(\bar{F}/F)$-conjugates of an element α of $\bar{F}$ can be distinguished from the elements of $\bar{F}$ that are not conjugate to α, by means of the minimal polynomial of α. We show in this section how the $\mathrm{Aut}(L/F)$-conjugates of an element α of L can be distinguished using a couple (f, g) of polynomials in $F[t]$. We do not know a reference for these results, although the techniques used are standard in the theory of field extensions.

Definition 6.1.1. Let K be a field, $\mathrm{Aut}(K)$ its automorphism group. If F is a subfield of K, then $\mathrm{Aut}(K/F)$ denotes those automorphisms of K which fix all elements of F.

We say that two elements $\alpha, \beta \in K$ are $\mathrm{Aut}(K)$-*conjugates*, if there exists a $\varphi \in \mathrm{Aut}(K)$, such that $\varphi(\alpha) = \beta$. We will also denote this with $\beta \in \mathrm{Aut}(K)(\alpha)$, meaning that β is in the orbit of α under the action of $\mathrm{Aut}(K)$ on K.

Proposition 6.1.2. *Let F be a field, L a separable algebraic extension of F. Let M be a field and let $\psi : F \hookrightarrow M$ be an embedding of F in M. Suppose that for each finite extension K of F in L, there exists an embedding $\chi : K \hookrightarrow M$, such that $\chi|_F = \psi$. Then there exists an embedding $\varphi : L \hookrightarrow M$ such that $\varphi|_F = \psi$.*

Proof. This is a variation of [Lan84, Chapter VII, Theorem 2.8]. One needs to apply Zorn's Lemma to the partially ordered set

$$\mathcal{F} = \{(K, \chi) \mid F \subseteq K \subseteq L, \chi : K \hookrightarrow M, \chi|_F = \psi, \\ \chi \text{ extends to all finite extensions of } K \text{ in } L\},$$

with the partial ordering $(K_1, \chi_1) \leq (K_2, \chi_2)$ if $K_1 \subseteq K_2$ and $\chi_2|_{K_1} = \chi_1$. By assumption, we have that $F \in \mathcal{F}$, so $\mathcal{F}$ is not empty.
Let $\{(K_i, \chi_i) \mid i \in I\}$ be a non-empty chain (a totally ordered subset) in $\mathcal{F}$. Let $K = \cup K_i$ and define χ on K to be equal to χ_i on each K_i. Because of the ordering on $\mathcal{F}$, χ is well defined. To prove that (K, χ) is in $\mathcal{F}$, let E/K be a finite extension, $E \subseteq L$. Let $\alpha \in L$ such that $E = K(\alpha)$, and $f(t)$ the minimal polynomial of α over K. Then there exists a K_i such that $f(t) \in K_i[t]$. Let $E_i = K_i(\alpha)$. Since χ_i extends to E_i, $\chi_i(f) = \chi(f)$ has a zero β in M. This means that χ extends to E, by sending α to β.
By Zorn's lemma, we find a maximal element (P, ρ) in $\mathcal{F}$. Suppose $P \neq L$, then there exists a finite extension N/P in L such that ρ extends to N and all finite extensions of N (because those are finite extensions of P), contradicting the maximality of (P, ρ). This proves there exists an extension of ψ to L. □

Theorem 6.1.3. *Let F be a field, L a separable algebraic extension of F and $\alpha \in L$. There exist polynomials $f(t), g(t) \in F[t]$ with g irreducible, such that the system*

$$\begin{cases} f(t) = \beta \\ g(t) = 0 \end{cases} \tag{6.1}$$

(with a parameter $\beta \in L$) has a solution $t \in L$ if and only if $\beta = \varphi(\alpha)$ for some $\varphi \in \mathrm{Aut}(L/F)$.

Proof. In this proof, we consider F as base field. All fields we mention are extensions of F and all morphisms are the identity on F.

Let $K = F(\alpha)$. This is a finite extension, so K has finitely many embeddings φ_1, $\ldots$, φ_n into L. For each of these embeddings, we define a finite extension $N_i \subseteq L$ of K: if φ_i extends to an automorphism of L, then $N_i := K$. If it does not extend, it follows from Proposition 6.1.2 that there exists a finite extension N_i/K such that φ_i does not extend to an embedding of N_i into L. Let N be a finite extension of F inside L containing all N_i. By the construction of N, we have that if an embedding $\varphi_i : K \hookrightarrow L$ extends to an embedding $\psi_i : N \hookrightarrow L$, then φ_i extends to an automorphism $\tilde{\varphi}_i$ of L (remark that $\tilde{\varphi}_i$ does not need to be equal to ψ_i on N).

Now choose any $\gamma \in N$ such that $N = F(\gamma)$. Let $g(t)$ be the minimal polynomial (over F) of γ and let $f(t)$ be such that $\alpha = f(\gamma)$. By construction, (6.1) has a solution $t = \gamma$ for $\beta = \alpha$. Since the system is $\mathrm{Aut}(L/F)$-invariant, it will have a solution for all $\beta \in \mathrm{Aut}(L/F)(\alpha)$.

Conversely, assume $\xi \in L$ satisfies (6.1) for a parameter $\beta \in L$. Since γ and ξ have the same minimal polynomial (namely $g(t)$) over F, there is an embedding $\psi : N \hookrightarrow L$ mapping γ to ξ. Let φ be the restriction of ψ to $K = F(\alpha)$. Then

$$\varphi(\alpha) = \varphi(f(\gamma)) = f(\psi(\gamma)) = f(\xi) = \beta.$$

The embedding $\varphi : K \hookrightarrow L$ obviously extends to the embedding ψ of N into L. Because of the construction of N, this implies that φ extends to an automorphism $\tilde{\varphi}$ of L. We conclude that $\tilde{\varphi}(\alpha) = \beta$, where $\tilde{\varphi} \in \mathrm{Aut}(L/F)$. □

Remark 6.1.4. If L/F is a Galois extension, then we can take $f(t) = t$ and g the minimal polynomial of α in Theorem 6.1.3. In this sense, one can say that the couple (f, g) refines the minimal polynomial because it can be used to characterize the $\mathrm{Aut}(L/F)$-conjugates of elements of L. However, there is no notion of uniqueness or minimality (this is because there is no unique choice for the extensions N_i/K in the proof of Theorem 6.1.3).

6.2 Automorphism-recursive fields

Let L be a recursive algebraic extension of $\mathbb{Q}$. In this section, we introduce automorphism-recursive fields. Such fields have the property that, given $\alpha \in L$, we can compute the set $\mathrm{Aut}(L/F)(\alpha)$, with F a number field in L. To do this, we will use the polynomials f and g appearing in Theorem 6.1.3.

Suppose we have a given $\alpha \in L$. For every β in the algebraic closure $\bar{L}$ with the same minimal polynomial as α over $\mathbb{Q}$ (this means α and β are $\mathrm{Aut}(\bar{L})$-conjugates), there are three possible cases:

1. $\beta \in L$ and $\beta = \varphi(\alpha)$ for some $\varphi \in \mathrm{Aut}(L)$;
2. $\beta \in L$ but $\beta \neq \varphi(\alpha)$ for all $\varphi \in \mathrm{Aut}(L)$;
3. $\beta \notin L$.

Let L be an algebraic extension of $\mathbb{Q}$, with recursive presentation $\sigma : L \tilde{\to} \mathbb{N}$.

For $\alpha \in L$, let $p_\alpha \in \mathbb{Q}[t]$ denote the minimal polynomial of α. Given $\sigma(\alpha) \in \mathbb{N}$, we can compute p_α. More precisely, we can compute the codes (under σ) of the coefficients of p_α. To do this, we try all monic irreducible polynomials in $\mathbb{Q}[t]$, until we find an $f(t)$ for which $f(\alpha) = 0$. Checking whether a polynomial over $\mathbb{Q}$ is irreducible can be done algorithmically, see for instance [Coh93, Section 3.5].

Definition 6.2.1. Let L be an algebraic extension of $\mathbb{Q}$. We call L *automorphism-recursive* if for every recursive presentation $\sigma : L \tilde{\to} \mathbb{N}$, there exists an algorithm with input $n \in \mathbb{N}$, and with output the natural numbers n_1 and n_2, such that if $\sigma(\alpha) = n$ for $\alpha \in L$, then n_1 is the number of roots in L of the minimal polynomial p_α, and n_2 the number of different $\mathrm{Aut}(L)$-conjugates of α.

Saying that L is automorphism-recursive is equivalent to saying that we can count the number of elements β in the three cases mentioned above.

Examples 6.2.2. We give some examples of automorphism-recursive fields.

1. Let L be the real closure of $\mathbb{Q}$, then L is automorphism-recursive. Since $\mathrm{Aut}(L/\mathbb{Q}) = 1$, we have $n_2 = 1$. To compute n_1, there exist real-root counting algorithms, for example using Sturm sequences (see [Coh93, Algorithm 4.1.11]).

2. Let L be the p-adic closure of $\mathbb{Q}$ for some prime p, that is the field of elements of $\mathbb{Q}_p$ that are algebraic over $\mathbb{Q}$. Since $\mathrm{Aut}(L/\mathbb{Q}) = 1$ (see [Lan84, Chapter XII, Exercise 3]), we have that $n_2 = 1$. To compute n_1, we can use repeatedly Nerode's algorithm in [Ner63] that decides whether a given polynomial has a zero in $\mathbb{Q}_p$.

3. Let $L/\mathbb{Q}$ be Galois and suppose that L is a recursive field. Then L is automorphism-recursive, because then $n_1 = n_2 = \deg p_\alpha$.

4. If $L/\mathbb{Q}$ is a finite extension, then L is automorphism-recursive because we can simply compute the finitely many automorphisms of L as linear maps of the finite dimensional $\mathbb{Q}$-vector space L.

Recall that Theorem 6.1.3 with $F = \mathbb{Q}$ stated that there exist polynomials $f(t), g(t) \in \mathbb{Q}[t]$ such that the system $f(t) = \beta, g(t) = 0$ has a solution if and only if $\beta \in \mathrm{Aut}(L)(\alpha)$. These polynomials can be effectively computed.

Proposition 6.2.3. *Let L be an automorphism-recursive algebraic extension of $\mathbb{Q}$ and fix a recursive presentation $\sigma : L \tilde{\to} \mathbb{N}$. Then we can compute, given $\sigma(\alpha)$ for some $\alpha \in L$, polynomials $f(t), g(t) \in \mathbb{Q}[t]$ satisfying Theorem 6.1.3 with $F = \mathbb{Q}$.*

Proof. We loop over all triples $(f(t), g(t), \gamma) \in \mathbb{Q}[t] \times \mathbb{Q}[t] \times L$ and look for those such that $f(\gamma) = \alpha$, $g(\gamma) = 0$ and g is irreducible. If we find such a triple, we compute all roots $\xi_1, \ldots, \xi_n$ in L of g. These can be enumerated since we know the number of roots of $g = p_\gamma$ by our hypothesis that L is automorphism-recursive. Let $\beta_i := f(\xi_i)$ and count the number of different β_i's (it is possible that $\beta_i = \beta_j$ even if $\xi_i \neq \xi_j$). Clearly, the $\mathrm{Aut}(L)$-conjugates of α appear amongst the β_i's. If the number of different β_i's equals this number of conjugates (which we know again by hypothesis), we are done and output $(f(t), g(t))$.

This algorithm always finishes because Theorem 6.1.3 guarantees the existence of such polynomials. □

This has as a corollary than we can compute all $\mathrm{Aut}(L/F)$-conjugates of $\alpha \in L$, with F a number field in L, even using different recursive presentations.

Theorem 6.2.4. *Let L be an automorphism-recursive algebraic extension of $\mathbb{Q}$. Consider two recursive presentations $\sigma, \tau : L \tilde{\to} \mathbb{N}$. There exists an algorithm which takes as input $\sigma(\alpha)$, $\sigma(\zeta)$ and $\tau(\zeta)$ for some $\alpha, \zeta \in L$ and outputs the set*

$$\{\tau(\beta) \in \mathbb{N} \mid \beta \in \mathrm{Aut}(L/\mathbb{Q}(\zeta))(\alpha)\}.$$

Proof. Let $F := \mathbb{Q}(\zeta)$ and $N := \mathbb{Q}(\zeta, \alpha) \subseteq L$. We first find an $\varepsilon \in N$ such that $N = \mathbb{Q}(\varepsilon)$. This can be done for example by enumerating the triples $(k, z(t), a(t)) \in \mathbb{Q} \times \mathbb{Q}[t] \times \mathbb{Q}[t]$ until $\zeta = z(\zeta + k\alpha)$ and $\alpha = a(\zeta + k\alpha)$ and then letting $\varepsilon = \zeta + k\alpha$. Since $\mathbb{Q}(\zeta, \alpha)$ has only finitely many subfields, [Lan84, Chapter VII, Theorem 6.1] guarantees that this will work. We use the recursive presentation σ for this computation.

Using Proposition 6.2.3, we compute $f(t), g(t) \in \mathbb{Q}[t]$ for ε. Now, we loop over all $\xi \in L$ (using the recursive presentation τ) to find all zeros of $g(t)$. For each ξ such that $g(\xi) = 0$, compute $\eta = f(\xi)$. Then $\eta = \varphi(\varepsilon)$ for some $\varphi \in \mathrm{Aut}(L)$ and we will find all elements of $\mathrm{Aut}(L)(\varepsilon)$ this way. Since $z(\varepsilon) = \zeta$, it follows that φ is the identity on F if and only if $z(\eta) = \zeta$. If indeed $z(\eta) = \zeta$, then $a(\eta) = \varphi(\alpha)$ with $\varphi \in \mathrm{Aut}(L/F)$ and we output $\tau(a(\eta))$. □

We can now generalize Proposition 6.2.3 to the relative situation, over a base number field F.

Theorem 6.2.5. *Let L be an automorphism-recursive algebraic extension of $\mathbb{Q}$ and fix a recursive presentation $\sigma : L \tilde{\to} \mathbb{N}$. Then we can compute, given $\sigma(\alpha)$ and $\sigma(\zeta)$ for some $\alpha, \zeta \in L$, polynomials $f(t), g(t) \in F[t]$ satisfying Theorem 6.1.3 with $F = \mathbb{Q}(\zeta)$.*

Proof. Start by applying Theorem 6.2.4 to compute the set $\mathrm{Aut}(L/F)(\alpha)$. Now loop over all 4-tuples $(f(t), g(t), g_0(t), \gamma) \in F[t] \times F[t] \times \mathbb{Q}[t] \times L$ and look for those such that $f(\gamma) = \alpha$, $g(\gamma) = 0$, $g \mid g_0$ and g is irreducible. If we find such a tuple, we compute all roots $\xi_1, \ldots, \xi_n$ in L of g_0. Consider only those roots ξ_i which are also roots of g. If $f(\xi_i) \in \mathrm{Aut}(L/F)(\alpha)$ for all those roots, then we output $(f(t), g(t))$ and we are done. □

The next proposition is a generalization of Theorem 6.2.4 to the polynomial ring $L[t]$. As mentioned in Examples 5.2.2, the polynomial ring $L[t]$ is recursive (given that L is recursive). And the recursive presentation of $L[t]$ can be chosen such that we can go back and forth between L and $L[t]$ in a recursive way. We extend the action of $\mathrm{Aut}(L)$ to the elements of $L[t]$ by acting on the coefficients: we define $\varphi(t) = t$ for $\varphi \in \mathrm{Aut}(L)$.

Theorem 6.2.6. *Let L be an automorphism-recursive, algebraic extension of $\mathbb{Q}$. Suppose $\sigma : L[t] \tilde{\to} \mathbb{N}$ and $\tau : L[t] \tilde{\to} \mathbb{N}$ are recursive presentations of the polynomial ring $L[t]$. There exists an algorithm which takes as input $\sigma(a)$, $\sigma(\zeta)$ and $\tau(\zeta)$ for some $a(t) \in L[t]$ and $\zeta \in L$ and outputs the set*

$$\{\tau(b) \in \mathbb{N} \mid b(t) = \varphi(a(t)) \text{ for some } \varphi \in \mathrm{Aut}(L/\mathbb{Q}(\zeta))\}.$$

Proof. Suppose $a(t) = \alpha_n t^n + \cdots + \alpha_1 t + \alpha_0$ and let $K = \mathbb{Q}(\alpha_0, \ldots, \alpha_n)$ be the number field generated by the coefficients of a. Let $\varepsilon \in L$ such that $K = \mathbb{Q}(\varepsilon)$. This implies that $a(t) \in \mathbb{Q}(\varepsilon)[t]$, so there exists a polynomial $h(t, u) \in \mathbb{Q}[t, u]$ such that $a(t) = h(t, \varepsilon)$. We can find such an h and ε simply by enumerating the elements of $\mathbb{Q}[t, u] \times L$. We use the recursive presentation σ for this, so we actually get $\sigma(\varepsilon)$.

We have that $\varphi(a(t)) = h(t, \varphi(\varepsilon))$ for $\varphi \in \mathrm{Aut}(L/\mathbb{Q}(\zeta))$. By Theorem 6.2.4, given $\sigma(\varepsilon)$, $\sigma(\zeta)$ and $\tau(\zeta)$, we can enumerate all $\tau(\varphi(\varepsilon))$ for $\varphi \in \mathrm{Aut}(L/\mathbb{Q}(\zeta))$. We then output the set of all $\tau(h(t, \varphi(\varepsilon)))$. □

6.3 Sets that are recursively enumerable for every recursive presentation

In this section, L is an automorphism-recursive, algebraic extension of $\mathbb{Q}$. We will give an algebraic characterization of the sets $\mathcal{S} \subseteq L$ that are r.e. for every recursive presentation of L. Namely, we will prove in Theorem 6.3.2 that they are the r.e. sets $\mathcal{S} \subseteq L$ for which there exists a finite extension $F/\mathbb{Q}$ such that $\mathcal{S}$ is invariant as a set under $\mathrm{Aut}(L/F)$. This theorem is formulated for r.e. subsets of L, but also holds for the polynomial ring $L[t]$.

One can easily see that this characterization holds for diophantine sets: suppose $\mathcal{S} \subseteq L$ is a diophantine set with defining polynomial $f(a, x_1, \ldots, x_n)$. If $F/\mathbb{Q}$ is the number field generated by the coefficients of f, then $\mathcal{S}$ is invariant as a set under $\mathrm{Aut}(L/F)$.

Lemma 6.3.1. *Let $L/\mathbb{Q}$ be an algebraic extension. Then there exists a chain $\mathbb{Q} = E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots$ of finite extensions $E_i/\mathbb{Q}$, such that $L = \cup_{i\geq 0} E_i$ and such that for every i, $\psi(E_i) = E_i$ for each $\psi \in \mathrm{Aut}(L)$.*

Proof. There exists a bijection $\sigma : L \tilde{\to} \mathbb{N}$. Let $L_0 = \mathbb{Q}$ and for $i \geq 1$ we let $L_i = \mathbb{Q}(\sigma^{-1}(1), \ldots, \sigma^{-1}(i))$. Then clearly $L_0 \subseteq L_1 \subseteq \ldots$ is an ascending chain of finite extensions $L_i/\mathbb{Q}$ such that $L = \cup_{i\geq 0} L_i$. Now let $\alpha_i \in L$ such that $L_i = \mathbb{Q}(\alpha_i)$, and let $E_i = \mathbb{Q}(\{\varphi(\alpha_i) \mid \varphi \in \mathrm{Aut}(L)\})$. Then $E_0 \subseteq E_1 \subseteq \ldots$ satisfies the thesis of the lemma. □

Theorem 6.3.2. *Let L be an automorphism-recursive, algebraic extension of $\mathbb{Q}$. Let $\mathcal{S} \subseteq L$, such that $\mathcal{S}$ is r.e. for some recursive presentation $\sigma : L \tilde{\to} \mathbb{N}$. Then $\mathcal{S}$ is r.e. for every recursive presentation $\tau : L \tilde{\to} \mathbb{N}$ if and only if there exists a finite extension $F/\mathbb{Q}$ such that $\mathcal{S}$ is invariant (as a set) under* $\mathrm{Aut}(L/F)$.

Proof. Suppose there is a finite extension $F/\mathbb{Q}$ such that $\mathcal{S}$ is invariant under $\mathrm{Aut}(L/F)$. After enlarging F with its $\mathrm{Aut}(L)$-conjugates, we may assume without loss of generality that $\psi(F) = F$ for all $\psi \in \mathrm{Aut}(L)$. Let $F = \mathbb{Q}(\zeta)$.

Let σ and τ be given recursive presentations of L. We consider σ, τ and F as part of the input data, so the algorithm will depend on these. This implies we know $\sigma(\zeta)$ and $\tau(\zeta)$.

We give an algorithm which runs over all elements of $\sigma(\mathcal{S})$ and outputs all elements of $\tau(\mathcal{S})$. This goes as follows: for every $a \in \sigma(\mathcal{S})$, let $\alpha = \sigma^{-1}(a) \in L$ and use Theorem 6.2.4 to output the set $\tau(\mathrm{Aut}(L/F)(\alpha))$. Since $\mathrm{Aut}(L/F)(\alpha) \subseteq \mathcal{S}$, we will eventually output the set $\tau(\mathcal{S})$ this way.

Now suppose that $\mathcal{S}$ is r.e. for every recursive presentation but that for every finite extension $F/\mathbb{Q}$, $\mathcal{S}$ is not invariant under $\mathrm{Aut}(L/F)$. Take such a recursive presentation τ. For every automorphism φ of L, $\tau \circ \varphi$ is also a recursive presentation of L. The idea is that we will construct a set $A \subseteq \mathrm{Aut}(L)$ of cardinality $2^{\aleph_0}$,

such that $\varphi(\mathcal{S}) \neq \psi(\mathcal{S})$ for different elements $\varphi \neq \psi$ of A. When τ runs over the $\varphi(S)$ with $\varphi \in A$, we will find uncountably many r.e. sets in $\mathbb{N}$, a contradiction.

From Lemma 6.3.1, it follows that there exist $E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots$, finite extensions $E_i/\mathbb{Q}$, such that $L = \cup_{i\geq 0} E_i$ and such that for every i, $\psi(E_i) = E_i$ for each $\psi \in \mathrm{Aut}(L)$. By assumption, for every i, $\mathrm{Aut}(L/E_i)(\mathcal{S}) \neq \mathcal{S}$. So let $\varphi_i \in \mathrm{Aut}(L/E_i)$, such that $\varphi_i(\mathcal{S}) \neq \mathcal{S}$. From this follows that there exists a finite extension K/E_i, such that $\varphi_i(\mathcal{S} \cap K) \neq \mathcal{S} \cap K$. Since there exists a $j > i$, such that $K \subseteq E_j$, we have that $\varphi_i(\mathcal{S} \cap E_j) \neq \mathcal{S} \cap E_j$. We now delete the intermediate fields $E_{i+1}, \ldots, E_{j-1}$ from our chain. In the resulting chain, E_j from the old chain becomes the new E_{i+1}. Summarizing, we have a chain $E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots$ of finite extensions $E_i/\mathbb{Q}$, such that $L = \cup_{i\geq 0} E_i$ such that for every i, $\psi(E_i) = E_i$ for each $\psi \in \mathrm{Aut}(L)$, and we have a $\varphi_i \in \mathrm{Aut}(L/E_i)$ such that $\varphi_i(\mathcal{S}) \neq \mathcal{S}$ and $\varphi_i(\mathcal{S} \cap E_{i+1}) \neq \mathcal{S} \cap E_{i+1}$.

We are now ready to define the set $A \subseteq \mathrm{Aut}(L/\mathbb{Q})$. Let I be a subset of $\mathbb{N}$, then we define $\varphi_I \in \mathrm{Aut}(L)$ as the composition of all φ_i with $i \in I$, and the order is such that $\varphi_{\mathbb{N}} = \cdots \circ \varphi_2 \circ \varphi_1 \circ \varphi_0$. So φ_I is an infinite product, but this is well defined since at each finite level $E_k/\mathbb{Q}$, there are only finitely many φ_i that act nontrivially, namely those with $i < k$ (by construction of the E_i). We now set $A = \{\varphi_I \in \mathrm{Aut}(L) \mid I \subseteq \mathbb{N}\}$.

Take different subsets I, J of $\mathbb{N}$. We have to prove that $\varphi_I(\mathcal{S}) \neq \varphi_J(\mathcal{S})$. Let i be the minimal natural number in which I and J differ, without loss of generality, we can assume that $i \in I \setminus J$. Consider $\varphi_I \circ \varphi_J^{-1}$, on $\mathcal{S} \cap E_{i+1}$ this works as φ_i. From this follows that $\varphi_I(\mathcal{S} \cap E_{i+1}) \neq \varphi_J(\mathcal{S} \cap E_{i+1})$, so $\varphi_I(\mathcal{S}) \neq \varphi_J(\mathcal{S})$. □

This last theorem was stated for the field L, but the same statement also holds for $L[t]$ (recall that $\varphi(t) = t$ for $\varphi \in \mathrm{Aut}(L)$). The proof is essentially the same, instead of Theorem 6.2.4, we would use Theorem 6.2.6.

6.4 Some examples of non automorphism-recursive fields

In section 6.2, we proved that in an automorphism-recursive field L, given two recursive presentations $\sigma, \tau : L \xrightarrow{\sim} \mathbb{N}$, and given $\sigma(\alpha)$ for some $\alpha \in L$, we can compute the set $\{\tau(\varphi(\alpha)) \mid \varphi \in \mathrm{Aut}(L)\}$. On the other hand, if for every element $\alpha \in L$, we can compute $\{\tau(\varphi(\alpha)) \mid \varphi \in \mathrm{Aut}(L)\}$ and we can compute the number of roots of its minimal polynomial p_α in L, it follows that L is automorphism-recursive. One can also ask if it is enough to be able to compute $\{\tau(\varphi(\alpha)) \mid \varphi \in \mathrm{Aut}(L)\}$, to conclude that L is automorphism-recursive. The answer to this is no, as we will show in our first construction, where we will construct a field H where for every $\alpha \in H$, we can compute $\{\tau(\varphi(\alpha)) \mid \varphi \in \mathrm{Aut}(H)\}$, but H is not automorphism-recursive. In our second construction, we will make a field M, that is also not automorphism-recursive, and we give recursive presentations $\sigma, \tau : M \xrightarrow{\sim} \mathbb{N}$, such that given $\sigma(\alpha)$, with $\alpha \in M$, we can not even compute the set $\{\tau(\varphi(\alpha)) \mid \varphi \in \mathrm{Aut}(M)\}$.

6.4.1 Discriminants

We will make our examples of fields that are not automorphism-recursive as a compositum of number fields K_i, $i \in \mathbb{N}$. Since we need to be able to determine the automorphisms of this compositum, we want the number fields K_i to be linearly disjoint over $\mathbb{Q}$. To do this, we use discriminants of number fields, a concept that we recall in this section. We also prove a preparatory Proposition 6.4.7 on linearly disjointness, to pave the way for the construction of our examples. For more background on discriminants and the related ramification behaviour, we refer to [Neu92, Chapter III, Section 2].

Definition 6.4.1. Let K be a field, $\bar{K}$ a fixed algebraic closure. Let $f \in K[t]$ be a monic polynomial with roots $\alpha_1, \ldots, \alpha_n \in \bar{K}$. We denote the discriminant of f with $\Delta(f) := \prod_{i<j}(\alpha_i - \alpha_j)^2$.

Definition 6.4.2. Let K/F be a finite separable extension with $[K : F] = n$. We define the discriminant of elements $\alpha_1, \ldots, \alpha_n \in K$ to be $\Delta(\alpha_1, \ldots, \alpha_n) = \det(\varphi_i(\alpha_j))^2$, where φ_i, $i = 1, \ldots, n$ are the F-embeddings of K in $\bar{K}$.

One easily sees that $\Delta(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{T}(\alpha_i \alpha_j))$, with $\mathrm{T} : K \to F$ the trace of the extension K/F.

Definition 6.4.3. Let K be a number field, and $\alpha_1, \ldots, \alpha_n$ a basis for $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Then the discriminant of K is $\Delta(K) = \Delta(\alpha_1, \ldots, \alpha_n)$.

The discriminant of K does not depend on the choice of $\mathbb{Z}$-basis. It is also well known that $|\Delta(K)| > 1$ for every number field $K \neq \mathbb{Q}$ (see [Neu92, Chapter III, Minkowski's Theorem 2.17]).

Definition 6.4.4. Let K/F be a number field extension with $[K : F] = n$. The (relative) discriminant $\Delta(K/F)$ is the ideal in $\mathcal{O}_F$ generated by $\Delta(\alpha_1, \ldots, \alpha_n)$ as $(\alpha_1, \ldots, \alpha_n)$ varies over all n-tuples in $\mathcal{O}_K$.

When $F = \mathbb{Q}$, then $\Delta(K/\mathbb{Q}) = (\Delta(K))$ (the principal ideal in $\mathbb{Z}$ generated by the absolute discriminant $\Delta(K)$).

Lemma 6.4.5. *Let K be a number field. Let $f(t) \in \mathcal{O}_K[t]$ be a monic irreducible polynomial of degree d and $L = K[t]/(f(t))$. Then $\Delta(f) \in \Delta(L/K)$.*

Proof. Let $x \in \mathcal{O}_L$ be a zero of f, then $\{1, x, x^2, \ldots, x^{d-1}\}$ is a basis for L/K with elements in $\mathcal{O}_L$. By definition, $\Delta(1, x, \ldots, x^{d-1}) \in \Delta(L/K)$. Let φ_i, $i \in \{1, \ldots, d\}$ be the K-embeddings $L \to \bar{K}$. Then

$$\Delta(1, x, \ldots, x^{d-1}) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x^{\varphi_1} & x^{\varphi_2} & \ldots & x^{\varphi_d} \\ \vdots & \vdots & \ddots & \vdots \\ (x^{d-1})^{\varphi_1} & (x^{d-1})^{\varphi_2} & \ldots & (x^{d-1})^{\varphi_d} \end{vmatrix} = \prod_{i<j} (x^{\varphi_i} - x^{\varphi_j})^2 = \Delta(f),$$

so $\Delta(f) \in \Delta(L/K)$. □

Lemma 6.4.6. *Let F be a number field. Let $f(t) \in \mathcal{O}_F[t]$ be a monic irreducible polynomial and let L be the splitting field of f over F. If $\mathfrak{p}$ is a prime of F such that $\mathfrak{p} \mid \Delta(L/F)$, then $\mathfrak{p} \mid (\Delta(f))$.*

Proof. We proceed by induction on the degree d of f. If $d = 1$, the assertion is trivial. Now suppose the statement is true for polynomials of degree strictly

smaller than d. Let $K = F[t]/(f(t))$. If K is the splitting field of f over F, then it follows immediately from Lemma 6.4.5 that if $\mathfrak{p}$ is a prime of F such that $\mathfrak{p} \mid \Delta(K/F)$, then $\mathfrak{p} \mid (\Delta(f))$. So suppose now that $g(t) \in \mathcal{O}_K[t]$ is a monic irreducible factor of f over K with $\deg g > 1$. From [Neu92, Chapter III, Corollary 2.10] follows that

$$\Delta(L/F) = \Delta(K/F)^{[L:K]} \, \mathrm{N}_{K/F}(\Delta(L/K)).$$

By the induction hypothesis, we have that if $\mathfrak{B}$ is a prime such that $\mathfrak{B} \mid \Delta(L/K)$, then $\mathfrak{B} \mid \Delta(g)\mathcal{O}_K$. Since $\Delta(f)\mathcal{O}_K \subseteq \Delta(g)\mathcal{O}_K$, we have that $\mathfrak{B} \mid \Delta(f)\mathcal{O}_K$. Since the primes in $\mathrm{N}_{K/F}(\Delta(L/K))$ lie below the primes of $\Delta(L/K)$, and from Lemma 6.4.5 we have that $\Delta(f) \in \Delta(K/F)$, it follows that the only primes in $\Delta(L/F)$ are primes that occur in $\Delta(f)\mathcal{O}_F$. □

Proposition 6.4.7. *Let $E/\mathbb{Q}$ be a finite extension. Let $\alpha \in \mathcal{O}_E$. Let $a, b \in \mathbb{R}$ with $a < b$. Then there exist infinitely many $r \in \mathbb{Q}$ such that*

1. *$\alpha - r$ is not a square in E,*
2. *$a < r < b$,*

and the quadratic extensions $E(\sqrt{\alpha - r})$ are all different.

Let $F/\mathbb{Q}$ be a finite Galois extension with $(\Delta(F), \Delta(E)) = 1$. Then we can find $r \in \mathbb{Q}$ such that also:

3. *F and $E(\sqrt{\alpha - r})$ are linearly disjoint over $\mathbb{Q}$.*

Proof. Since there are infinitely many primes that split completely in E ([Neu92, Chapter VII, Corollary 13.6]), there are infinitely many prime numbers p_i such that

(i) p_i splits completely in E,
(ii) $p_i \neq 2$,
(iii) $p_i\mathcal{O}_E + \alpha\mathcal{O}_E = \mathcal{O}_E$.

We show that for every prime p_i, $i \in \mathbb{N}$, that satisfies conditions (i)–(iii), we can find $r_i \in \mathbb{Q}$ such that $\alpha - r_i$ is not a square in E, $a < r_i < b$, and the extensions $E(\sqrt{\alpha - r_i})$ are all different. We do this inductively, so r_i depends on all primes $p_1, p_2, \ldots, p_i$.

Suppose that $p_i O_E = \mathfrak{p}_1 \ldots \mathfrak{p}_n$. For the remainder of the proof, we fix a prime $\mathfrak{p} \mid p_i$. We have that $O_E/\mathfrak{p} \cong \mathbb{F}_{p_i}$. Because of condition (iii), $\overline{\alpha} \in \mathbb{F}_{p_i}^*$. Let $\overline{\varepsilon_i} \in \mathbb{F}_{p_i}^*$ such that $\overline{\alpha} - \overline{\varepsilon_i}$ is not a square in $\mathbb{F}_{p_i}^*$. For all $j \in \mathbb{N}$, $j < i$, let $\overline{\delta_j} \in \mathbb{F}_{p_j}^*$ such that $\overline{\alpha} - \overline{\delta_j}$ is a square in $\mathbb{F}_{p_j}^*$.

By weak approximation [EP05, Theorem 1.1.3] follows that there exists an $r_i \in \mathbb{Q}$ such that $a < r_i < b$ and

$$\begin{cases} r_i \equiv \overline{\varepsilon_i} \mod p_i \\ r_i \equiv \overline{\delta_j} \mod p_j \qquad \text{for all } j = 1, \ldots, i-1. \end{cases}$$

So $\overline{\alpha - r_i} = \overline{\alpha} - \overline{\varepsilon_i}$ is not a square in $\mathbb{F}_{p_i}^*$, therefore $\alpha - r_i$ is not a square in E.

Suppose that $E(\sqrt{\alpha - r_j}) = E(\sqrt{\alpha - r_i})$ with $j < i$. Then $\alpha - r_j$ and $\alpha - r_i$ are in the same square class of E, and so for the prime $\mathfrak{p} \mid p_j$, $\alpha - r_j$ and $\alpha - r_i$ are in the same square class in $O_E/\mathfrak{p} \cong \mathbb{F}_{p_j}$. This is a contradiction, since $\overline{\alpha - r_j}$ is not a square in $\mathbb{F}_{p_j}^*$, but $\overline{\alpha - r_i}$ is a square in $\mathbb{F}_{p_j}^*$. Therefore, the extensions $E(\sqrt{\alpha - r_i})$ are all different.

Let $K = F \cap E$. From [Neu92, Chapter III, Corollary 2.10] follows that $\Delta(F/\mathbb{Q}) \subseteq \Delta(K/\mathbb{Q})$ and $\Delta(E/\mathbb{Q}) \subseteq \Delta(K/\mathbb{Q})$. Since $(\Delta(F), \Delta(E)) = 1$, it follows that $\Delta(K/\mathbb{Q}) = 1$, so $K = \mathbb{Q}$.

Suppose that $\mathbb{Q} \subsetneq F \cap E(\sqrt{\alpha - r_i})$. Let $\beta \in F \cap E(\sqrt{\alpha - r_i})$ such that $F \cap E(\sqrt{\alpha - r_i}) = \mathbb{Q}(\beta)$. Then $\beta \notin E$, so $E(\beta) = E(\sqrt{\alpha - r_i})$ or equivalently

$$(F \cap E(\sqrt{\alpha - r_i}))E = E(\sqrt{\alpha - r_i}).$$

Since F has only finitely many subfields, this gives only finitely many different extensions $E(\sqrt{\alpha - r_i})$. Therefore, there exists an r_ℓ such that $F \cap E(\sqrt{\alpha - r_\ell}) = \mathbb{Q}$. Since $F/\mathbb{Q}$ is Galois, it follows from [Lan84, Chapter VIII, Theorem 1.12] that F and $E(\sqrt{\alpha - r_\ell})$ are linearly disjoint over $\mathbb{Q}$. □

6.4.2 Construction of the examples

Let $n \in \mathbb{N}$ and $p_n(t) = t^3 + 3t^2 - nt - 4$, then the discriminant of p_n is $\Delta(p_n) = n(4n^2+9n+216)$. So if $n > 0$, then $p_n(t)$ has three different real roots $x_n, y_n, z_n \in \mathbb{R}$. Without loss of generalization, we may suppose that $x_n < y_n < z_n$.

From now on, we only consider $n \in \mathbb{N} \setminus \{0, 2, 5, 8, 27\}$, so $p_n(t)$ is irreducible over $\mathbb{Q}$.

We computed that the only rational point on the elliptic curve $E : y^2 = n(4n^2 + 9n + 216)$ is the point $(0, 0)$, so for all $n \in \mathbb{Q}^*$, $\Delta(p_n)$ is not a square. Therefore $\mathbb{Q}(z_n)/\mathbb{Q}$ is not Galois.

For the construction of our examples, it suffices that for $n \in \mathbb{N}$ sufficiently large, $\Delta(p_n)$ is not a square. So if one does not want to rely on a computation, one could also use Siegel's Theorem ([Sil86, Chapter IX, Corollary 3.2.1]), from which follows that the set of integral points on E is finite.

We have that $\Delta(p_1) = 229$ and $\Delta(p_3) = 837$. Using the Chinese Remainder Theorem, one can prove the following lemma.

Lemma 6.4.8. *Given $N \in \mathbb{N}$, with $N > 0$, there exists an $x \in \mathbb{N} \setminus \{0, 2, 5, 8, 27\}$, such that* $\gcd(N, \Delta(p_x)) = 1$.

Proof. Consider the following congruences:

$$\begin{cases} x \equiv 1 \mod p & \text{for all primes } p \text{ such that } p \mid N, p \neq 229 \\ x \equiv 3 \mod 229. \end{cases}$$

From the Chinese Remainder Theorem follows there exists a solution $x \in \mathbb{N} \setminus \{0, 2, 5, 8, 27\}$. Let p be a prime, $p \mid N$ and $p \neq 229$. Then $\Delta(p_x) \equiv \Delta(p_1) \equiv 229 \not\equiv 0 \mod p$, hence $p \nmid \Delta(p_x)$. Furthermore $\Delta(p_x) \equiv \Delta(p_3) \equiv 837 \mod 229$, so $229 \nmid \Delta(p_x)$. This gives $\gcd(N, \Delta(p_x)) = 1$. □

Let $E_n := \mathbb{Q}(x_n, y_n, z_n)$. From Proposition 6.4.7 follows that there exists an $r_1 \in \mathbb{Q}$ such that $y_1 < r_1 < z_1$ and $z_1 - r_1$ is not a square in $E_1 = \mathbb{Q}(x_1, y_1, z_1)$. Again applying this Proposition 6.4.7, gives $q_1 \in \mathbb{Q}$ such that $x_1 < q_1 < y_1$ and $y_1 - q_1$

is not a square in $E_1(\sqrt{z_1 - r_1})$. Let $L_1 := \mathbb{Q}(x_1, y_1, z_1, \sqrt{z_1 - r_1}, \sqrt{y_1 - q_1})$, and $N_1/\mathbb{Q}$ the Galois closure of L_1. Let $a_1 := 1$. We now describe how we construct inductively the field L_{a_k} for every $k \in \mathbb{N}$, $k \geq 2$.

Let $N_{a_{k-1}}/\mathbb{Q}$ be the Galois closure of $L_{a_1}L_{a_2}\dots L_{a_{k-1}}$. From Lemma 6.4.8 follows that there exists an $a_k \in \mathbb{N} \setminus \{0, 2, 5, 8, 27\}$, such that $(\Delta(N_{a_{k-1}}), \Delta(p_{a_k})) = 1$. From Lemma 6.4.6 follows that that $(\Delta(N_{a_{k-1}}), \Delta(E_{a_k})) = 1$. Applying Lemma 6.4.7 twice, we find $r_{a_k}, q_{a_k} \in \mathbb{Q}$ such that $x_{a_k} < q_{a_k} < y_{a_k} < r_{a_k} < z_{a_k}$, $z_{a_k} - r_{a_k}$ is not a square in E_{a_k}, $y_{a_k} - q_{a_k}$ is not a square in $E_{a_k}(\sqrt{z_{a_k} - r_{a_k}})$, and such that $N_{a_{k-1}}$ and L_{a_k} are linearly disjoint over $\mathbb{Q}$, with $L_{a_k} := E_{a_k}(\sqrt{z_{a_k} - r_{a_k}}, \sqrt{y_{a_k} - q_{a_k}})$. Therefore $L_{a_1}\dots L_{a_{k-1}}$ and L_{a_k} are linearly disjoint over $\mathbb{Q}$.

Let $A = \{a_k \mid k \in \mathbb{N}\}$. Since there is a recursive bijection of A to $\mathbb{N}$, there exists a subset $S \subseteq A$ that is recursively enumerable but not recursive.

Construction 1

We keep the notation from before, so $\bar{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$,

$$E_n = \mathbb{Q}(x_n, y_n, z_n) \quad \text{and} \quad L_n = E_n(\sqrt{z_n - r_n}, \sqrt{y_n - q_n}),$$

and $S \subset A$ is r.e. but its complement is not r.e. Let

$$F_n = \begin{cases} \mathbb{Q}(z_n, \sqrt{z_n - r_n}) & \text{if } n \in A \setminus S \\ L_n & \text{if } n \in S. \end{cases}$$

Construct the field extension $H/\mathbb{Q}$ as the compositum of all F_n where n runs through A.

Proposition 6.4.9. *The field H is recursive.*

Proof. We give an algorithm that constructs H as a chain of fields $H_1 := \mathbb{Q} \subset H_2 \subset H_3 \subset \dots$ such that $H = \cup_i H_i$. Let a background algorithm $\mathcal{A}$ run, that prints the elements of S. Now we describe our algorithm step by step. In step 1, we let $H_1 = \mathbb{Q}$. In step $2n$, we let $H_{2n} := H_{2n-1}\mathbb{Q}(z_n, \sqrt{z_n - r_n})$ for $n \in A$, and $H_{2n} := H_{2n-1}$ if $n \in \mathbb{N} \setminus A$. We keep a list of the $\mathbb{Q}(z_n, \sqrt{z_n - r_n})$ that we add. In step $2n + 1$ of our algorithm, if $k \in S$ is printed in step n of algorithm $\mathcal{A}$, we let

$H_{2n+1} := H_{2n}L_k$. Otherwise, set $H_{2n+1} := H_{2n}$. From [FS56, Theorem 6.12] follows that this gives a recursive presentation $\sigma : H \tilde{\to} \mathbb{N}$. □

Proposition 6.4.10. *Let $\varphi \in \mathrm{Aut}(H)$. If $n \in S$, then $\varphi|_{E_n} = id|_{E_n}$, $\varphi(\sqrt{z_n - r_n}) = \pm\sqrt{z_n - r_n}$ and $\varphi(\sqrt{y_n - q_n}) = \pm\sqrt{y_n - q_n}$.*

Proof. Let $\varphi \in \mathrm{Aut}(H)$. Suppose that $\varphi(z_n) = y_n$. Then $\varphi(\sqrt{z_n - r_n}) \in H$ is a root of $t^2 - (y_n - r_n)$. Since H is a subfield of $\mathbb{R}$ and $y_n - r_n < 0$, this is a contradiction. Suppose that $\varphi(z_n) = x_n$, then again $\varphi(\sqrt{z_n - r_n}) \in H$ is a root of $t^2 - (x_n - r_n)$, this also gives a contradiction. So $\varphi(z_n) = z_n$, and $\varphi(\sqrt{z_n - r_n}) = \pm\sqrt{z_n - r_n}$. Suppose that $\varphi(y_n) = x_n$. Then $\varphi(\sqrt{y_n - q_n})$ is a root of $t^2 - (x_n - q_n)$. Since $x_n - q_n < 0$, this gives again a contradiction. So $\varphi(y_n) = y_n$, $\varphi(x_n) = x_n$ and $\varphi(\sqrt{y_n - q_n}) = \pm\sqrt{y_n - q_n}$. □

From this Proposition 6.4.10 follows that if $n \in S$, the two $\mathrm{Aut}(\bar{\mathbb{Q}})$-conjugates of z_n are in H, but they are not $\mathrm{Aut}(H)$-conjugate to z_n. So for z_n, the number of $\mathrm{Aut}(H)$-conjugates is always 1, but the number of roots of its minimal polynomial p_n in H is 3 if and only if $n \in S$. So if H would be automorphism-recursive, then we would have an algorithm that gives the number of roots of p_n in H for every $n \in A$, so that decides whether $n \in S$. Therefore, H is not automorphism-recursive.

However, let σ, τ be two recursive presentations of H. Given $\sigma(a)$, we show that we can compute the set $\{\tau(\varphi(a)) \mid \varphi \in \mathrm{Aut}(H)\}$.

We illustrate this first in the case that a has minimal polynomial p_n, for some $n \in A$. Then given $\sigma(a)$, we have to show that we can compute $\tau(a)$. This can be done as follows. Let $p_n(t) = (t-a)q_n(t)$ and consider the algorithm that runs over all $b \in H$ and checks two things: whether b is a root of $t^2 - (a - r_n)$ and whether b is a root of q_n. Since a is a root of p_n, either $a = z_n$, and then we must find a root of $t^2 - (a - r_n)$, or $a \neq z_n$, and then we must find a root of q_n, so eventually the algorithm halts. Suppose we find a root of $t^2 - (a - r_n)$, then we know $a = z_n$, and we output $\tau(z_n)$. Suppose we find a root of q_n, then we know the three roots a, b, c of p_n are in H. Then we go on and search for a root of $t^2 - (a - r_n), t^2 - (a - q_n), t^2 - (b - r_n), t^2 - (b - q_n), t^2 - (c - r_n)$ or $t^2 - (a - q_n)$ for both representations σ and τ. Eventually, we will be able to determine $\sigma(x_n), \sigma(y_n), \sigma(z_n)$ and also $\tau(x_n), \tau(y_n), \tau(z_n)$. Given that $a \in \{x_n, y_n, z_n\}$, this suffices to determine $\tau(a)$ from $\sigma(a)$.

Now we treat the general case for $\alpha \in H$, with minimal polynomial p_α not one of the p_n. Then there exists a finite set $B \subset A$ such that

$$\alpha \in \mathbb{Q}(\{x_n, y_n, z_n, \sqrt{z_n - r_n}, \sqrt{y_n - q_n} \mid n \in B\}) = F.$$

So α can be written as a polynomial in the generators of the finite extension $F/\mathbb{Q}$, let $\alpha = f(\{x_n, y_n, z_n, \sqrt{z_n - r_n}, \sqrt{y_n - q_n} \mid n \in B\})$, with the coefficients of f in $\mathbb{Q}$. We already gave an algorithm to compute $\tau(x_n), \tau(y_n)$ and $\tau(z_n)$. To compute $\tau(\pm\sqrt{z_n - r_n})$ and $\tau(\pm\sqrt{y_n - q_n})$, we just compute the roots in H of $t^2 - (z_n - r_n)$ and $t^2 - (y_n - q_n)$ for τ. Because of the linear disjointness property, the $\mathrm{Aut}(H)$-conjugates of α are all the possible $f(\{x_n, y_n, z_n, \pm\sqrt{z_n - r_n}, \pm\sqrt{y_n - q_n} \mid n \in B\})$.

Construction 2

We keep the same notations as in the first construction. We construct the field extension $M/\mathbb{Q}$ as the compositum of $\mathbb{Q}(z_n)$ if $n \in A \setminus S$, and L_n if $n \in S$. A similar proof as in Proposition 6.4.9, gives a recursive presentation $\sigma : M \tilde{\to} \mathbb{N}$. Just as in Proposition 6.4.10, we see that for every $\varphi \in \mathrm{Aut}(M)$, $\varphi(z_n) = z_n$ for every $n \in A$, and that for $n \in S$, $\varphi(y_n) = y_n, \varphi(x_n) = x_n, \varphi(\sqrt{z_n - r_n}) = \pm\sqrt{z_n - r_n}$ and $\varphi(\sqrt{y_n - q_n}) = \pm\sqrt{y_n - q_n}$.

In the same way, we construct the field extension $M'/\mathbb{Q}$ as the compositum of $\mathbb{Q}(y_n)$ if $n \in A \setminus S$, and L_n if $n \in S$. Similarly as in Proposition 6.4.9, one can prove that this is also a recursive field. Let $\tau : M' \tilde{\to} \mathbb{N}$ be a recursive presentation. We define an isomorphism $\psi : M \to M'$, by letting $\psi(z_n) = y_n$ if $n \in A \setminus S$, and $\psi(z_n) = z_n$ if $n \in S$. If $L_n \subset M$, then we let $\psi|_{L_n} = id|_{L_n}$.

Now consider the recursive presentations $\sigma : M \tilde{\to} \mathbb{N}$ and $\tau \circ \psi : M \tilde{\to} \mathbb{N}$, and suppose that for every $m \in M$, given $\sigma(m)$, we could compute the set $\{(\tau \circ \psi)(\varphi(m)) \mid \varphi \in \mathrm{Aut}(M)\}$. Consider the algorithm that takes as input a natural number $n \in A$, and then computes $\sigma(z_n)$, which can be done since the function $A \to \mathbb{N} : n \mapsto \sigma(z_n)$ is recursive. The algorithm then computes $(\tau \circ \psi)(z_n)$ (this is possible by assumption). Since the function $A \to \mathbb{N} : n \mapsto \tau(y_n)$ is also recursive, the algorithm can then determine whether $\tau(\psi(z_n)) = \tau(y_n)$. Since $\tau(\psi(z_n)) = \tau(y_n)$ if and only if $n \in A \setminus S$, this is a contradiction.

Chapter 7

Recursively enumerable sets are diophantine

With the preparatory work in the previous chapter, we can now finish the proof that recursively enumerable sets in $L[t]$ that are r.e. for every recursive presentation, are diophantine. This proof follows some of the structure of the proof in [Dem07a] that recursively enumerable sets in $O_L[t]$ (with L a totally real algebraic extension of $\mathbb{Q}$), that are r.e. for every recursive presentation, are diophantine. Our proof is based on Section 6.3, Lemma 6.10 and Section 6.6 of [Dem07a]. However, we will also need that $\mathbb{Z}[t]$ is diophantine in $L[t]$. From [Dem10, Theorem 3.1] follows that this is the case if the predicate "$\deg a(t) \leq \deg b(t)$" is diophantine. We give a diophantine definition of the degree for two classes of fields, namely real fields and subfields of p-adic fields.

7.1 Diophantine definition of degree

As before, L is an algebraic extension of $\mathbb{Q}$, and $L[t]$ the polynomial ring in one variable over L. In this section, we give a diophantine definition of the predicate "$\deg a(t) \leq \deg b(t)$" with $a(t), b(t) \in L[t]$, $a \neq 0$ and $b \neq 0$, for two classes of fields L. We handle the case that L can be embedded in $\mathbb{R}$ and the case that L can

be embedded in a finite extension of $\mathbb{Q}_p$.

7.1.1 For algebraic subfields of the reals

We recall some definitions concerning real fields.

Definition 7.1.1. A field K is called a *(formally) real field* if -1 is not a sum of squares in K.

A field K is real if and only if K is an ordered field, this means there exists a subset P (the positive elements) of K such that if $\alpha, \beta \in P$ then $\alpha + \beta \in P$ and $\alpha\beta \in P$, $P \cap (-P) = \{0\}$ and $P \cup (-P) = K$. A real field can have more than one ordering P.

In this section, L is a real, algebraic extension of $\mathbb{Q}$. The orderings P on L correspond exactly to the embeddings $\varphi : L \hookrightarrow \mathbb{R}$. Namely, if $\varphi : L \hookrightarrow \mathbb{R}$ is an embedding, then $P = \{\alpha \in L \mid \varphi(\alpha) \geq 0\}$ is an ordering on L. And converse, if P is an ordering on L, then there exists an embedding of L into the real closure of $\mathbb{Q}$, hence an embedding $L \hookrightarrow \mathbb{R}$.

Definition 7.1.2. A rational function $a(t) \in L(t)$ is called *positive-definite* on L if $\varphi(a(\xi)) \geq 0$ for all $\xi \in L$ on which a is defined, and for all embeddings $\varphi : L \hookrightarrow \mathbb{R}$. We denote this with $a \geq 0$, the notation $a \geq b$ is equivalent with $a - b \geq 0$.

Proposition 7.1.3. *The set of positive-definite polynomials in $L[t]$ is diophantine.*

Proof. Let $a(t) \in L[t]$ be a positive-definite polynomial. Let $\tilde{P}$ be an ordering on $L(t)$. The restriction $P := \tilde{P}|_L$ corresponds to an embedding $\varphi : L \hookrightarrow \mathbb{R}$. Then $\varphi(a(\xi)) \geq 0$ for all $\xi \in L$. Since L is dense its real closure, this is equivalent with $\varphi(a(\xi)) \geq 0$ for all ξ in the real closure of L. From the Artin-Schreier theorem (see for instance [Pfi95, Chapter 6, Theorem 2.3]) follows that there exist finitely many $\pi_i \in L$ such that $\varphi(\pi_i) \geq 0$ and $f_i \in L(t)$ such that

$$a = \sum_i \pi_i f_i^2.$$

It follows that $a \in \tilde{P}$. This holds for every ordering $\tilde{P}$ of $L(t)$. Therefore, a is a sum of squares in $L(t)$ ([Pfi95, Chapter 6, Corollary 1.8]).

Now, let F be the number field generated by the coefficients of $a(t)$. From a theorem of Pourchet (see [Pou71]) follows that $a(t)$ is a sum of at most 5 squares in $F(t)$. So we have

$a(t) \in L[t]$ is positive-definite $\Leftrightarrow (\exists a_1, \ldots, a_5, b \in L[t])(b \neq 0 \wedge b^2 a = a_1^2 + \cdots + a_5^2)$.

Since the nonzero elements in $L[t]$ are diophantine in $L(t)$ (Section 2.1, Example 3), this definition of the positive-definite polynomials is diophantine. □

Theorem 7.1.4. *Let L be a real, algebraic extension of $\mathbb{Q}$. Let $a(t), b(t) \in L[t]$, $a \neq 0$ and $b \neq 0$. Then*

$$\deg a(t) \leq \deg b(t) \Leftrightarrow (\exists \rho, \pi \in L)\ a^2 \leq \rho + \pi b^2.$$

Proof. Let $\deg a(t) = n, \deg b(t) = m$, $a(t) = \alpha_n t^n + \cdots + \alpha_0$ and $b(t) = \beta_m t^m + \cdots + \beta_0$. Let F be a number field containing all the coefficients α_i and β_i.

Suppose first that $n \leq m$. Then we need to prove that $\varphi(a(\xi)^2) \leq \varphi(\rho + \pi b(\xi)^2)$ for every $\xi \in L$ and every embedding $\varphi : L \hookrightarrow \mathbb{R}$. If $n = m$, we choose $\pi \in \mathbb{Q}$ such that $\varphi(\alpha_n^2) < \pi\varphi(\beta_n^2)$ for every real embedding φ. This is possible, since there are only finitely many embeddings of F in $\mathbb{R}$. If $n < m$, we set $\pi = 1$. In both cases, the polynomial $\varphi(a^2 - \pi b^2)$ has even degree with a negative leading term. Therefore, $\varphi(a^2 - \pi b^2)$ reaches a maximum $m_\varphi \in \mathbb{R}$. We now take $\rho \in \mathbb{Q}$ such that $\rho \geq m_\varphi$ for every embedding $\varphi : F \hookrightarrow \mathbb{R}$. As before, this is possible since there are only finitely many such embeddings. It follows that $\varphi(a^2 - \pi b^2) \leq \rho$.

For the converse, we choose one particular real embedding of L. Suppose that there exist $\rho, \pi \in L$ such that $\varphi(a^2) \leq \varphi(\rho + \pi b^2)$. Since the left hand side is a positive definite polynomial of degree $2n$, dominated by a polynomial of degree at most $2m$, it follows that $n \leq m$. □

7.1.2 For algebraic subfields of p-adic fields

In this section, we let L be an algebraic subfield of a p-adic field. Let $a(t), b(t) \in L[t]$, $a \neq 0$ and $b \neq 0$. Then $\deg a \leq \deg b$ is equivalent with $v_\infty(a/b) \geq 0$.

Since we proved in Corollary 4.1.6 that "$v_\infty \geq 0$" is diophantine, this gives us a diophantine definition of the degree. This idea appeared before in Demeyer's article [Dem10], where he proves that recursively enumerable sets over $K[t]$, with K a number field, are diophantine. Since every number field can be embedded in a nondyadic p-adic field, he uses Kim and Roush's diophantine definition of the valuation ring in $K(t)$, with K a subfield of a nondyadic p-adic field in [KR95], to give a diophantine definition of the degree.

Theorem 7.1.5. *Let L be a subfield of a p-adic field that is algebraic over $\mathbb{Q}$. The relation "$\deg a(t) \leq \deg b(t)$" with $a(t), b(t) \in L[t]$, $a \neq 0$ and $b \neq 0$ is diophantine in $L[t]$.*

Proof. Let $a(t), b(t) \in L[t] \setminus \{0\}$, we have that $\deg b - \deg a = v_\infty(a/b)$. From Corollary 4.1.6 follows that in $L(t)$, the relation $v_\infty(a/b) \geq 0$ is diophantine. Since the nonzero elements in $L[t]$ are diophantine in $L(t)$ (Section 2.1, Example 3), it follows that "$\deg a(t) \leq \deg b(t)$" is diophantine in $L[t]$. □

7.2 Recursively enumerable sets are diophantine

As before, L is an algebraic extension of $\mathbb{Q}$, and $L[t]$ the polynomial ring in one variable over L. We work in a fixed algebraic closure $\bar{L}$ of L.

Lemma 7.2.1. *Let F be a number field and L an algebraic field extension of F. Suppose that $\mathbb{Z}[t]$ is diophantine over $L[t]$. Then $F[t]$ is diophantine over $L[t]$.*

Proof. Let $\alpha \in L$ such that $F = \mathbb{Q}(\alpha)$, and let $d = [F : \mathbb{Q}]$. Then $a(t) \in F[t]$ if and only if there exist $b \in \mathbb{Z} \setminus \{0\}$ and $a_0(t), \ldots, a_{d-1}(t) \in \mathbb{Z}[t]$ such that

$$ba(t) = a_0(t) + a_1(t)\alpha + \cdots + a_{d-1}(t)\alpha^{d-1}.$$

Since $\mathbb{Z}\setminus\{0\}$ is diophantine in $\mathbb{Z}[t]$ (it is r.e.), and $\mathbb{Z}[t]$ is by assumption diophantine over $L[t]$, it follows that $F[t]$ is diophantine over $L[t]$. □

Definition 7.2.2. A *bounding predicate* for $L[t]$ is a relation $\delta(a, n)$ with $a(t) \in L[t]$ and $n \in \mathbb{N}$ such that:

1. For any fixed $n \in \mathbb{N}$, there are only finitely many $a \in L[t]$ that satisfy $\delta(a, n)$.

2. If $\mathcal{B}$ is a finite subset of $L[t]$, then there exists an $n \in \mathbb{N}$ such that $\delta(b, n)$ holds for every $b \in \mathcal{B}$.

We call a bounding predicate *effective* if the following also holds:

3. There exists an algorithm, with input $n \in \mathbb{N}$, that produces a finite set $\mathcal{B}_n \subset \bar{L}[t]$, such that $\mathcal{B}_n \cap L[t]$ is exactly the set of the $b \in L[t]$ that satisfy $\delta(b, n)$.

To make sense of this last condition, we use the known fact that $\bar{L}$ is a recursive field with a recursive embedding of L into $\bar{L}$, see [Rab60, Theorem 7]. More precisely, if ι denotes the embedding $L \hookrightarrow \bar{L}$ and σ is a recursive presentation of L, then there exists a recursive presentation $\tau : \bar{L} \tilde{\to} \mathbb{N}$ such that $\tau \circ \iota \circ \sigma^{-1} : \mathbb{N} \to \mathbb{N}$ is a recursive function. However, in general, the image $\iota(L)$ of this function (as a subset of $\bar{L}$) is not recursive. In other words, given an element of $\bar{L}$, we cannot decide whether it belongs to L.

We now give a diophantine effective bounding predicate for $L[t]$.

Lemma 7.2.3. *Let L be an algebraic extension of $\mathbb{Q}$, and suppose that $\mathbb{Z}[t]$ is diophantine over $L[t]$. Let $\sigma : \mathbb{Z}[t] \tilde{\to} \mathbb{N}$ be a recursive presentation, and let $p_n(t) = \sigma^{-1}(n)$ if $\sigma^{-1}(n)$ is nonzero and $p_{\sigma(0)}(t) = 1$. Let $\delta(a, n)$ be the relation "$a(t)t + 1 \mid p_n(t)$". Then δ is an effective bounding predicate for $L[t]$ that is diophantine over $L[t]$.*

Proof. Fix $n \in \mathbb{N}$ and consider $p_n(t)$, which is a nonzero polynomial. As a polynomial in $L[t]$, it has only finitely many divisors, up to units. If we force the constant coefficient of such a divisor to be 1, there are only finitely many possibilities, so only finitely many values for $a(t)$.

Given finitely many polynomials $a_1(t), \ldots, a_m(t) \in L[t]$, we define

$$q(t) = \prod_i (a_i(t)t + 1).$$

Let K denote the number field generated by the coefficients of q, then $r(t) = \mathrm{N}_{K/\mathbb{Q}}(q(t))$ is an element of $\mathbb{Q}[t]$. Finally, we multiply $r(t)$ with a nonzero integer to clear all denominators to get a nonzero polynomial $s(t) = d \cdot r(t) \in \mathbb{Z}[t]$. Let $n = \sigma(s)$. We conclude that $a_i(t)t + 1 \mid q(t) \mid r(t) \mid s(t) = p_n(t)$ for all i.

The bounding predicate is effective because we can easily factor $p_n(t)$ in $\bar{L}[t]$ (search for all the zeros by trying every element of $\bar{L}$). Then we can compute all divisors of $p_n(t)$ and normalize them such that the constant coefficient becomes 1, skipping those divisors with constant coefficient 0. For each divisor $a(t)t + 1$, we output $a(t)$.

Finally, we show that it is diophantine. Consider the set $\mathcal{S} = \{(p_n(t), n) \in \mathbb{Z}[t] \times \mathbb{N}\}$ as subset of $\mathbb{Z}[t] \times \mathbb{Z}[t]$. By definition, this set is r.e. if and only if $\{(\sigma(p_n(t)), \sigma(n)) \in \mathbb{N} \times \mathbb{N}\}$ is r.e. If we ignore $n = \sigma(0)$ and $n = \sigma(1)$ for simplicity, this set is equal to $\{(n, \sigma(n)) \in \mathbb{N} \times \mathbb{N}\}$. Since we can easily compute $\sigma(n)$ for any n (it suffices to know $\sigma(1)$), it follows that $\mathcal{S}$ is a recursively enumerable (even recursive) subset of $\mathbb{Z}[t] \times \mathbb{Z}[t]$. By [Den78b], this is also a diophantine subset of $\mathbb{Z}[t] \times \mathbb{Z}[t]$. Using the assumption that $\mathbb{Z}[t]$ is diophantine over $L[t]$ gives us that $\mathcal{S}$ is diophantine over $L[t]$. Since divisibility is obviously diophantine, this shows that the predicate $\delta(a, n)$: $a(t)t + 1 \mid p_n(t)$ is diophantine. □

We will now finish the proof of the main theorem.

Theorem 7.2.4. *Let L be an automorphism-recursive, algebraic extension of $\mathbb{Q}$. Suppose that $\mathbb{Z}[t]$ is diophantine over $L[t]$. Let $\mathcal{S} \subseteq L[t]$ be r.e. for every recursive presentation of $L[t]$. Then $\mathcal{S}$ is diophantine over $L[t]$.*

Proof. Since L is automorphism-recursive and $\mathcal{S}$ is r.e. for every recursive presentation of $L[t]$, by Theorem 6.3.2 we have that $\mathrm{Aut}(L/F)(\mathcal{S}) = \mathcal{S}$ for some finite extension F of $\mathbb{Q}$ in L.

We give an algorithm that codes the elements of $\mathcal{S}$ into a triple $(n, \omega, \alpha) \in \mathbb{N} \times F \times L$. We call the set of these triples $\mathcal{R}_1$. Given $a(t) \in \mathcal{S}$, let n be the smallest natural number for which $\delta(a, n)$ holds, with δ the bounding predicate from Lemma 7.2.3. Since by assumption $\mathbb{Z}[t]$ is diophantine over $L[t]$, from Lemma 7.2.3 follows that δ is effective. So we can find n algorithmically by computing $\mathcal{B}_n \subseteq \bar{L}[t]$ for increasing values of n until $a(t) \in \mathcal{B}_n$.

Next, let $d(t) = \prod_{b \in \mathcal{B}_n \setminus \{a\}} (a(t) - b(t))$, which is an element of $\bar{L}[t]$. Since d is not the zero polynomial, there exists an $\omega \in \mathbb{Q}$ such that $a(\omega) \neq b(\omega)$ for all $b \in \mathcal{B}_n \setminus \{a\}$. We know that ω exists, so we can try every $\omega \in \mathbb{Q}$ until we find one that works, and we let $\alpha = a(\omega)$.

Now we do a second encoding of the elements of $\mathcal{R}_1$ into a quadruple $(n, \omega, f(t), g(t)) \in \mathbb{N} \times F \times F[t] \times F[t]$. Given $(n, \omega, \alpha) \in \mathcal{R}_1$, we find $f(t), g(t) \in F[t]$ (see Theorem 6.2.5) such that the system

$$\begin{cases} f(t) = \alpha \\ g(t) = 0 \end{cases}$$

has a zero in L, but for every $\beta \in L$ with $\beta \notin \mathrm{Aut}(L/F)(\alpha)$ the system

$$\begin{cases} f(t) = \beta \\ g(t) = 0 \end{cases}$$

does not have a zero in L. The set of these quadruples $(n, \omega, f(t), g(t))$ will be called $\mathcal{R}$.

Since both these encodings are recursive procedures, the sets $\mathcal{R}_1$ and $\mathcal{R}$ are r.e. For the ring $F[t]$, we know that r.e. sets are diophantine (see [Dem10, Theorem 5.1]). So $\mathcal{R}$ is diophantine over $F[t]$. Since $\mathbb{Z}[t]$ is diophantine over $L[t]$, from Lemma 7.2.1 follows that $F[t]$ is diophantine in $L[t]$. Therefore $\mathcal{R}$ is diophantine over $L[t]$.

The final step is to give a diophantine definition of $\mathcal{S}$, given that $\mathcal{R}$ is diophantine. For this, we need to undo the two encodings using diophantine formulas.

We claim that:

$$a \in \mathcal{S} \tag{7.1}$$

$$\Updownarrow$$

$$(\exists\, n \in \mathbb{N})(\exists\, \omega \in F)(\exists\, f(t), g(t) \in F[t])(\exists\, \alpha, \gamma \in L)$$

$$(n, \omega, f(t), g(t)) \in \mathcal{R} \tag{7.2}$$

$$\wedge\ f(\gamma) = \alpha\ \wedge\ g(\gamma) = 0 \tag{7.3}$$

$$\wedge\ \delta(a, n) \wedge a(\omega) = \alpha. \tag{7.4}$$

First we prove that the definition is indeed diophantine. We have that L is diophantine in $L[t]$, since the constants in $L[t]$ are the invertible elements and 0. By

construction, the set $\mathcal{R}$ is diophantine over $L[t]$. From Lemma 7.2.1, it follows that $F[t]$ is diophantine over $L[t]$, and therefore F is also diophantine over $L[t]$.

If $a \in \mathcal{S}$, we take the corresponding $(n, \omega, \alpha) \in \mathcal{R}_1$ and $(n, \omega, f(t), g(t)) \in \mathcal{R}$. Then (7.2) is true and (7.3) and (7.4) follow from the construction of $\mathcal{R}_1$ and $\mathcal{R}$.

Conversely, assume (7.2), (7.3) and (7.4). Consider $(n, \omega, f(t), g(t)) \in \mathcal{R}$. This must come from some $(n, \omega, \beta) \in \mathcal{R}_1$, which in turn comes from some $b \in \mathcal{S}$. Since the system $f(t) = \alpha$ and $g(t) = 0$ has a solution $\gamma \in L$, we must have $\alpha = \varphi(\beta)$ for some $\varphi \in \mathrm{Aut}(L/F)$.

The construction of $\mathcal{R}_1$ implies that $\delta(b, n)$ holds, that $b(\omega) = \beta$ and that $b(\omega) \neq q(\omega)$ for all $q \neq b$ for which $\delta(q, n)$ holds. Applying φ^{-1} on (7.4) and considering $\omega \in F$, we get $\varphi^{-1}(a)(\omega) = \beta = b(\omega)$. Since $\delta(a, n)$ holds and δ is invariant under $\mathrm{Aut}(L/\mathbb{Q})$, also $\delta(\varphi^{-1}(a), n)$ holds.

All this implies that $b = \varphi^{-1}(a)$. Since $\mathrm{Aut}(L/F)(\mathcal{S}) = \mathcal{S}$ and $b \in \mathcal{S}$, we conclude that $a \in \mathcal{S}$. □

Corollary 7.2.5. *Let L be an automorphism-recursive, algebraic extension of $\mathbb{Q}$ and assume either that L is real, or that L can be embedded in a finite extension of $\mathbb{Q}_p$. Let $\mathcal{S} \subseteq L[t]$ be r.e. for every recursive presentation of $L[t]$. Then $\mathcal{S}$ is diophantine over $L[t]$.*

Proof. Using the hypotheses on the field L, we proved in Section 7.1 that "$\deg a(t) \leq \deg b(t)$" is diophantine, so from [Dem10, Theorem 3.1] follows that $\mathbb{Z}[t]$ is diophantine over $L[t]$. The result now follows from Theorem 7.2.4. □

Samenvatting

Inleiding

Het tiende probleem van Hilbert is één van de 23 wiskundige problemen die Hilbert opstelde in 1900. Een aantal van die problemen stelde hij voor in zijn befaamde toespraak op de conferentie in Parijs van het International Congress of Mathematics in 1900. Zijn bedoeling was dat deze problemen in de komende eeuw onderzocht zouden worden. De volledige lijst van 23 problemen werd later gepubliceerd, onder andere in [Hil00]. De originele formulering van het tiende probleem van Hilbert is als volgt.

Entscheidung der Lösbarkeit einer Diophantischen Gleichung. Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

Of in het Nederlands.

Bepalen of een diophantische vergelijking een oplossing heeft. Gegeven een diophantische vergelijking in een willekeurig aantal variabelen en met gehele coëfficiënten: *stel een procedure op zodat, na een eindig aantal operaties, beslist kan worden of de vergelijking een oplossing heeft over de gehele getallen.*

In hedendaagse terminologie zouden we zeggen dat het tiende probleem van Hilbert vraagt om een algoritme met als input een veelterm over $\mathbb{Z}$ in een willekeurig

aantal variabelen, en met output "ja" als de gegeven veelterm een oplossing in de gehele getallen heeft en "nee" als de veelterm geen gehele oplossing heeft. In 1970 bewees Matiyasevich de volgende stelling, verder bouwend op eerder werk van Davis, Putnam en Robinson.

Stelling (DPRM-stelling). *Een verzameling $A \subseteq \mathbb{Z}^k$ is recursief opsombaar als en slechts als A diophantisch is over $\mathbb{Z}$.*

We noemen deze stelling de DPRM-stelling, uit deze stelling volgt het negatieve antwoord op het tiende probleem van Hilbert, dus er bestaat geen algoritme dat beslist of diophantische vergelijkingen over $\mathbb{Z}$ een oplossing hebben.

Hilberts tiende probleem, en ook de sterkere DPRM-stelling kunnen voor andere ringen en velden geformuleerd worden (zie Sectie 2.1 en 5.1). In deze thesis geven we dergelijke resultaten: we bewijzen het negatieve antwoord op Hilberts tiende probleem voor rationale functievelden in één variabele over een p-adisch veld (dit is een eindige uitbreiding van een $\mathbb{Q}_p$). Wat betreft de DPRM-stelling, bewijzen we dat recursief opsombare verzamelingen die recursief opsombaar zijn voor elke recursieve presentatie, diophantisch zijn voor de veeltermring in één variabele over bepaalde algebraïsche uitbreidingen van $\mathbb{Q}$.

Een goed overzicht van de gekende resultaten en open problemen rond Hilberts tiende probleem kan gevonden worden in de overzichtsartikels [Phe94] en [PZ00]. Nog interessante overzichtsartikels die de relaties met andere problemen in getaltheorie en algebraïsche meetkunde verkennen zijn [Maz94] en [Shl00]. Er zijn ook twee goede inleidende teksten over Hilberts tiende probleem van Poonen, namelijk [Poo03] en [Poo08].

De resultaten over onbeslisbaarheid van diophantische vergelijkingen die tot hiertoe gekend zijn voor een domein R, reduceren allemaal tot het onbeslisbaarheidsresultaat voor $\mathbb{Z}$. Om deze reductie uit te voeren, probeert men een diophantisch model van de gehele getallen in R te vinden. Voor rationale functievelden $K(t)$ over een veld K volstaat het een diophantische definitie van de valuatiering van v_∞ te geven. Men gebruikt dan elliptische krommen om met deze definitie zo'n diophantisch model van de gehele getallen te construeren. Deze methode werd voor het eerst gebruikt door Denef ([Den78a]) in karakteristiek 0, algemeen kan het resultaat als volgt geformuleerd worden.

Stelling ([PZ00, Theorem 2.3]). *Zij K een veld en zij K_0 het priemveld van K. Zij t een transcendent element over K. Onderstel dat er een diophantische definitie $\psi(x)$ bestaat, zodat het volgende geldt:*

1. *voor alle $x \in K_0(t)$ zodat $v_\infty(x) \geq 0$, hebben we dat $\psi(x)$ geldt;*
2. *voor alle $x \in K(t)$ zodat $\psi(x)$ geldt, hebben we dat $v_\infty(x) \geq 0$.*

Dan zijn diophantische vergelijkingen over $K(t)$ onbeslisbaar.

Denef gebruikte deze methode om diophantische onbeslisbaarheid te bewijzen voor $K(t)$, met K een reëel veld. In [KR95] bewezen Kim en Roush onbeslisbaarheid voor $K(t)$, met K een deelveld van een p-adisch veld met oneven restklassenkarakteristiek. Wij verbeterden hun resultaat in [DD12], en gaven een bewijs van diophantische onbeslisbaarheid voor $K(t)$, met K een p-adisch veld dat ook dyadisch mag zijn. We pasten dit toe om diophantische onbeslisbaarheid te bewijzen voor $K(t)$, met K een algebraïsch deelveld van een p-adisch veld, eveneens zonder veronderstellingen over de karakteristiek van het restklassenveld. In positieve karakteristiek p, werd diophantische onbeslisbaarheid voor $K(t)$, met K een eindig veld van karakteristiek p, bewezen door Pheidas in [Phe91] (p oneven), en door Videla in [Vid94] ($p = 2$). Kim en Roush bewezen diophantische onbeslisbaarheid voor $\mathbb{C}(t_1, t_2)$ in [KR92]. Het is een open probleem of diophantische vergelijkingen over $\mathbb{C}(t)$ onbeslisbaar zijn.

Zij nu $R[t]$ de veeltermring in één variabele over een domein R van karakteristiek 0. In [Den78a], bewees Denef dat Hilbert's tiende probleem voor $R[t]$ met coëfficiënten in $\mathbb{Z}[t]$ onbeslisbaar is. Later bewees hij het resultaat ook voor een domein van positieve karakteristiek p in [Den79] (met de coëfficiënten van de diophantische vergelijkingen in $(\mathbb{Z}/p\mathbb{Z})[t]$).

Als R een recursieve ring is, dan kunnen we het sterkere resultaat dat recursief opsombare verzamelingen diophantisch zijn beschouwen. Hierover is er veel minder geweten. In de eerste plaats is er het resultaat van Denef dat recursief opsombare verzamelingen diophantisch zijn voor de veeltermring $\mathbb{Z}[t]$ (zie [Den78b]). Deze methode werd veralgemeend door Zahidi, die de equivalentie aantoonde in [Zah99] voor $O_K[t_1, \ldots, t_n]$ met O_K de ring van gehelen in een totaal reëel getallenveld K, en door Demeyer in [Dem10] voor $R[t]$, met R een recursieve deelring

van een getallenveld. In karakteristiek p bewees Demeyer voor $K[t]$, met K een recursieve algebraïsche uitbreiding van een eindig veld, dat verzamelingen die recursief opsombaar zijn voor elke recursieve presentatie, diophantisch zijn, gebruik makend van zijn resultaat in [Dem07b] dat recursief opsombare verzamelingen diophantisch zijn voor $\mathbb{F}_q[t]$. Wij bewezen dat recursief opsombare verzamelingen die recursief opsombaar zijn voor elke recursieve presentatie, diophantisch zijn voor $L[t]$, met $L/\mathbb{Q}$ een automorfisme-recursieve algebraïsche uitbreiding, die kan ingebed worden in een reëel veld of in een p-adisch veld.

Overzicht

Deel I: Hilberts tiende probleem voor rationale functievelden

In deel I bewijzen we diophantische onbeslisbaarheid voor het rationale functieveld $K(t)$ over een p-adisch veld K (i.e. een eindige uitbreiding van een $\mathbb{Q}_p$) en ook over een algebraïsch deelveld K van een p-adisch veld. Dit veralgemeent een resultaat van Kim en Roush, die in [KR95] diophantische onbeslisbaarheid bewezen voor rationale functievelden over deelvelden van een p-adisch veld waarvan het restklassenveld oneven karakteristiek heeft. In deze thesis passen we hun methoden aan door meer in de context van de theorie van de kwadratische vormen te werken, en we geven een gezamenlijk bewijs voor zowel restklassenkarakteristiek p oneven als $p = 2$.

Deel I gaat van start met twee voorbereidende hoofdstukken. In het eerste hoofdstuk herhalen we de definitie van een valuatie en enkele basiseigenschappen. De valuaties waarmee we vooral werken in deze thesis zijn de p-adische valuaties en de valuaties op een rationaal functieveld $K(t)$ die triviaal zijn op K (desondanks zijn er bepaalde valuaties die de p-adische valuatie naar $K(t)$ uitbreiden (zie Sectie 1.3), die impliciet voorkomen in het bewijs van onze Hoofdstelling 3.3.1). We introduceren ook de Newton veelhoek, een meetkundig object dat de valuaties van de wortels van een veelterm geeft. In het tweede hoofdstuk geven we een inleiding op het tiende probleem van Hilbert, waarbij we ons concentreren op rationale functievelden. We geven het bewijs van Denef dat diophantische onbeslisbaarheid voor $K(t)$ reduceert tot het geven van een diophantische definitie van

de valuatiering van v_∞ in $K(t)$, voor $\operatorname{char} K = 0$. Op deze manier presenteren we in deze thesis een volledig zelf-omvattend bewijs van ons resultaat van diophantische onbeslisbaarheid voor $K(t)$, met K een p-adisch veld. Tenslotte vergelijken we de gekende resultaten over onbeslisbaarheid voor rationale functievelden.

In onze diophantische definitie van de valuatiering van v_∞ in $K(t)$ spelen kwadratische vormen een belangrijke rol. We moeten namelijk kunnen bewijzen of een bepaalde klasse van 7-dimensionale kwadratische vormen, waarvan de coëfficienten afhangen van een gegeven rationale functie, isotroop is. Daarom concentreert Hoofdstuk 3 zich volledig op kwadratische vormen, met eerst wat inleiding, en daarna de opbouw tot onze Hoofdstelling 3.3.1, die zegt dat als $g \in K[t]$ een bepaalde Newton veelhoek heeft dat dan een bepaalde 7-dimensionale vorm q, die afhangt van g, isotroop is over $K(t)$. Ons bewijs volgt wat van de structuur van het bewijs van Kim en Roush, maar zij bewijzen veel stellingen in hun artikel over kwadratische vormen door te reduceren naar het restklassenveld. Aangezien dit een rationaal functieveld is over een eindig veld van oneven karakteristiek, kunnen ze kwadratische wederkerigheid gebruiken, en het resultaat terug liften met Hensels Lemma. Omdat we een bewijs wilden dat ook werkt in restklassenkarakteristiek 2, konden we deze techniek niet gebruiken. Maar eigenlijk is het natuurlijker om de veeltermen over het p-adisch veld K te beschouwen, in plaats van de reductie ervan in het restklassenveld. Bijgevolg definiëren we in Sectie 3.2 een soort van kwadratisch wederkerigheidssymbool voor veeltermen over K, en we verifiëren een kwadratische wederkerigheidswet voor dit symbool.

In [KR95] bewijzen Kim en Roush ook dat de kwadratische vorm q isotroop is over rationale functievelden over algebraïsche deelvelden van niet-dyadische p-adische velden. In hun bewijs gaan ze naar een eindige uitbreiding van K, waar ze zich ontdoen van de dyadische priemen. Ze geven dus enkel een diophantische definitie van de valuatiering van v_∞ voor deelvelden van niet-dyadische p-adische velden, die aan bepaalde voorwaarden voldoen. Aangezien ze ook bewijzen dat elke deelveld van een niet-dyadisch p-adisch veld zo'n eindige uitbreiding met extra voorwaarden bezit, volstaat dit om Hilberts tiende probleem voor $K(t)$ te bewijzen, met K een deelveld van een niet-dyadisch p-adisch veld. Door ons vorig resultaat voor p-adische velden aan te wenden, vereenvoudigen en veralgemenen we dit bewijs ook zodat het voor alle priemen p geldt. In ons bewijs is het ook niet meer nodig om over te gaan op een eindige uitbreiding. We kunnen dus een diophantische definitie geven van de valuatiering van v_∞ voor alle

rationale functievelden in één variabele over een algebraïsch deelveld van een p-adisch veld. Dit wordt gedaan in Hoofdstuk 4, waar we ons resultaat over de isotropie van q gebruiken om een diophantische definitie te geven van het predicaat "$v_\infty(x)$ is even" voor $x \in K(t)$. Dit kan dan geherformuleerd worden tot een diophantische definitie van "$v_\infty(x) \geq 0$", wat impliciet gedaan wordt in Stelling 4.1.5.

Ons resultaat over diophantische onbeslisbaarheid voor $K(t)$, met K een p-adisch veld, werd gepubliceerd in [DD12].

Deel II: Diophantische verzamelingen over veeltermringen

Ons startpunt in dit deel is het werk van Demeyer in zijn doctoraatsthesis (zie [Dem07a]) voor veeltermringen over $\mathcal{O}_L$, met L een totaal reële algebraïsche uitbreiding van $\mathbb{Q}$. We onderzoeken wanneer recursief opsombare verzamelingen diophantisch zijn voor de veeltermring $L[t]$, met $L/\mathbb{Q}$ een recursieve, algebraïsche uitbreiding. Of een verzameling $\mathcal{S} \subseteq L[t]$ recursief opsombaar (r.o.) is, zou kunnen afhangen van de gekozen recursieve presentatie van $L[t]$. Daarentegen zijn diophantische verzamelingen r.o. voor elke recursieve presentatie. Verder is een diophantische verzameling invariant onder $\mathrm{Aut}(L/F)$, met $F/\mathbb{Q}$ de eindige uitbreiding voortgebracht door de definiërende vergelijking van de diophantische verzameling. Dus enkel recursief opsombare verzamelingen $\mathcal{S} \subseteq L[t]$ die recursief opsombaar zijn voor elke recursieve presentatie van $L[t]$ en die invariant zijn onder de automorfismes van een eindige uitbreiding van $\mathbb{Q}$, kunnen diophantisch zijn. In sectie 6.3 tonen we aan dat deze twee voorwaarden waaraan r.o. verzamelingen zouden moeten voldoen, eigenlijk equivalent zijn. Namelijk, een recursief opsombare verzameling $\mathcal{S}$ is recursief opsombaar voor elke recursieve presentatie als en slechts als er een eindige uitbreiding $F/\mathbb{Q}$ bestaat zodat $\mathcal{S}$ invariant is als verzameling onder $\mathrm{Aut}(L/F)$.

Om het hoofdresultaat van dit deel te bewijzen, namelijk dat recursief opsombare verzamelingen die r.o. zijn voor elke recursieve presentatie diophantisch zijn voor $L[t]$, met $L/\mathbb{Q}$ een recursieve algebraïsche uitbreiding, hadden we een extra voorwaarde nodig over de automorfismen van L. Dit bracht ons tot de definitie van een automorfisme-recursief veld. In een automorfisme-recursief veld L

kunnen we, gegeven een element $\alpha \in L$, het aantal wortels in L van de minimaalveelterm van α over F berekenen, en we weten hoeveel van deze wortels $\mathrm{Aut}(L/F)$-toegevoegd zijn aan α. We bewezen een aantal essentiële eigenschappen die een automorfisme-recursief veld heeft, bijvoorbeeld, gegeven een element $\alpha \in L$, weten we niet alleen het aantal $\mathrm{Aut}(L/F)$-toegevoegden van α, maar we kunnen deze ook berekenen. Om wat meer intuïtie te ontwikkelen voor het concept automorfisme-recursief veld, construeerden we ook velden die één van deze eigenschappen bezitten, maar die niet automorfisme-recursief zijn. Een andere belangrijke eigenschap die een automorfisme-recursief veld heeft, is dat we een koppel veeltermen over een getallenveld F in L dat de $\mathrm{Aut}(L/F)$-toegevoegden van een element $\alpha \in L$ karakteriseert, kunnen berekenen. Daarna gebruikten we deze veeltermen om de elementen van de recursief opsombare verzameling $\mathcal{S}$ met $\mathrm{Aut}(L/F)(\mathcal{S}) = \mathcal{S}$ op een diophantische manier te coderen. Om te bewijzen dat onze definitie van $\mathcal{S}$ diophantisch is, hadden we ook nodig dat $\mathbb{Z}[t]$ diophantisch is over $L[t]$.

In Stelling 7.2.4 bewijzen we het hoofdresultaat van dit deel, namelijk zij $L/\mathbb{Q}$ een automorfisme-recursief veld en veronderstel dat $\mathbb{Z}[t]$ diophantisch is over $L[t]$, dan zijn recursief opsombare verzamelingen in $L[t]$ die recursief opsombaar zijn voor elke recursieve presentatie, diophantisch.

Uit [Dem10] volgt dat dit zo is als het predicaat "$\deg a \leq \deg b$" voor $a, b \in L[t] \setminus \{0\}$ diophantisch is. In Hoofdstuk 7.1 geven we een diophantische definitie van de graad in het geval dat L ingebed kan worden in $\mathbb{R}$ en in het geval dat L ingebed kan worden in een p-adisch veld.

Samen met Jeroen Demeyer bereidden we een artikel over dit werk voor.

Bibliography

[BMS67] Hyman Bass, John Milnor, and Jean-Pierre Serre, *Solution of the congruence subgroup problem for* $\mathrm{SL}_n\,(n \geq 3)$ *and* $\mathrm{Sp}_{2n}\,(n \geq 2)$, Inst. Hautes Études Sci. Publ. Math. (1967), no. 33, 59–137.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, no. 138, Springer, 1993.

[DD12] Claudia Degroote and Jeroen Demeyer, *Hilbert's tenth problem for rational function fields over p-adic fields*, J. Algebra **361** (2012), 172–187.

[Dem07a] Jeroen Demeyer, *Diophantine sets over polynomial rings and Hilbert's tenth problem for function fields*, Ph.D. thesis, Ghent University, 2007.

[Dem07b] ———, *Recursively enumerable sets of polynomials over a finite field are Diophantine*, Invent. Math. **170** (2007), no. 3, 655–670.

[Dem10] ———, *Diophantine sets of polynomials over number fields*, Proc. Amer. Math. Soc. **138** (2010), no. 8, 2715–2728.

[Den78a] Jan Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399.

[Den78b] ———, *Diophantine sets over* $\mathbb{Z}[T]$, Proc. Amer. Math. Soc. **69** (1978), no. 1, 148–150.

[Den79] ———, *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium 78 (M. Boffa, D. van Dalen, and

K. Mcaloon, eds.), Studies in logic and the foundations of mathematics, no. 97, North-Holland, 1979, pp. 131–145.

[Eis07] Kirsten Eisenträger, *Hilbert's tenth problem for function fields of varieties over number fields and p-adic fields*, J. Algebra **310** (2007), no. 2, 775–792.

[EP05] Antonio Engler and Alexander Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer, 2005.

[FS56] Albrecht Fröhlich and John C. Shepherdson, *Effective procedures in field theory*, Phil. Trans. Roy. Soc. London **248** (1956), 407–432.

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, no. 52, Springer, 1977.

[Hil00] David Hilbert, *Mathematische Probleme*, Nachrichten von der Königl. Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-Physikalische Klasse **1** (1900), 253–297.

[KR92] Ki Hang Kim and Fred Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, J. Algebra **150** (1992), no. 1, 35–44.

[KR95] ———, *Diophantine unsolvability over p-adic function fields*, J. Algebra **176** (1995), no. 1, 83–110.

[Lam05] Tsit-Yuen Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, no. 67, American Mathematical Society, 2005.

[Lan73] Serge Lang, *Elliptic functions*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1973.

[Lan84] ———, *Algebra*, Advanced Book Program (Second ed.), Addison-Wesley Publishing Company, Reading, Massachusetts, 1984.

[Maz94] Barry Mazur, *Questions of decidability and undecidability in number theory*, J. Symbolic Logic **59** (1994), no. 2, 353–371.

[MB07] Laurent Moret-Bailly, *Sur la définissabilité existentielle de la non-nullité dans les anneaux*, Algebra & Number Theory **1** (2007), no. 3, 331–346.

[Ner63] Anil Nerode, *A decision method for p-adic integral zeros of diophantine equations*, Bull. Amer. Math. Soc. **69** (1963), 513–517.

[Neu92] Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, 1992.

[NSW00] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2000.

[Pfi95] Albrecht Pfister, *Quadratic forms with applications to Algebraic Geometry and Topology*, London Mathematical Society Lecture Note Series, vol. 127, Cambridge University Press, 1995.

[Phe91] Thanases Pheidas, *Hilbert's tenth problem for rational function fields over finite fields*, Invent. Math. **103** (1991), 1–8.

[Phe94] _____, *Extensions of Hilbert's tenth problem*, J. Symbolic Logic **59** (1994), no. 2, 372–397.

[Poo03] Bjorn Poonen, *Hilbert's tenth problem over rings of number-theoretic interest*, Arizona Winter School 2003 notes, `http://math.berkeley.edu/~poonen/papers/aws2003.pdf`, 2003.

[Poo08] _____, *Undecidability in number theory*, Notices Amer. Math. Soc. **55** (2008), no. 3, 344–350.

[Pou71] Yves Pourchet, *Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques*, Acta Arith. **19** (1971), 89–104.

[PZ00] Thanases Pheidas and Karim Zahidi, *Undecidability of existential theories of rings and fields: a survey*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (Ghent, 1999) (Denef et al., eds.), Contemp. Math., vol. 270, 2000, pp. 49–105.

[Rab60] Michael Rabin, *Computable algebra, general theory and theory of computable fields*, Trans. Amer. Math. Soc. **95** (1960), 341–360.

[Rei03] Irving Reiner, *Maximal orders*, London Mathematical Society Monographs, New Series, no. 28, Oxford University Press, 2003.

[Sch85] Winfried Scharlau, *Quadratic and hermitian forms*, Grundlehren Math. Wiss., no. 270, Springer Berlin, 1985.

[Ser80] Jean-Pierre Serre, *Corps locaux*, Actualités scientifiques et industrielles, Hermann, 1980.

[Shl00] Alexandra Shlapentokh, *Hilbert's tenth problem over number fields, a survey*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Contemp. Math., vol. 270, Amer. Math. Soc., Providence, RI, 2000, pp. 107–137.

[SHT99] Viggo Stoltenberg-Hansen and John V. Tucker, *Computable rings and fields*, Handbook of computability theory, Stud. Logic Found. Math., vol. 140, North-Holland, Amsterdam, 1999, pp. 363–447.

[Sil86] Joseph Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, no. 106, Springer, 1986.

[Vid94] Carlos Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc. **120** (1994), 249–253.

[Zah99] Karim Zahidi, *Existential undecidability for rings of algebraic functions*, Ph.D. thesis, Ghent University, 1999.

Index